ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT®

Advances in Mathematics 183 (2004) 209–239

ADVANCES IN Mathematics

http://www.elsevier.com/locate/aim

Invariants of finite Hopf algebras

Serge Skryabin*

Chebotarev Research Institute, Kazan, Russia

Received 30 October 2002; accepted 28 January 2003

Communicated by Pavel Etingof

Abstract

This paper extends classical results in the invariant theory of finite groups and finite group schemes to the actions of finite Hopf algebras on commutative rings. Topics considered include integrality over the invariant rings, properties of the canonical map between the prime spectra, orbital and stabilizer algebras, projectivity over the invariant rings, and descent of Cohen–Macaulayness.

Keywords: Hopf algebras; Invariant rings; Integral ring extensions; Going-down; Cohen–Macaulay rings

0. Introduction

This paper extends classical results in the invariant theory of finite groups and finite group schemes to the actions of finite Hopf algebras on commutative rings. Suppose that H is a finite-dimensional Hopf algebra and A a commutative algebra, say over a field K. Let $\delta : A \to A \otimes H$ be an algebra homomorphism which makes A into a right H-comodule. In this case A is called an H-comodule algebra. The coaction of H on A corresponds to an action of the dual Hopf algebra H^*. For technical reasons all results in this paper are formulated in terms of coactions. The situation where H is commutative can be described geometrically by giving an action of the finite group scheme $G = \operatorname{Spec} H$ on the scheme $X = \operatorname{Spec} A$. The subring of G-invariants $A^G \subset A$ represents then the quotient scheme X/G. A fact of fundamental importance states that A is an integral extension of A^G. In case of

*Corresponding author. Current address: Mathematisches Seminar, University of Hamburg, Bundesstr. 55, 20146 Hamburg, Germany.

E-mail address: fm1a009@math.uni-hamburg.de.

0001-8708/03/$ - see front matter
doi:10.1016/S0001-8708(03)00087-2

ordinary finite groups this classical result goes back to the work of E. Noether. The question of whether a similar assertion is true for a noncommutative H was posed by Montgomery [22, 4.2.6]. Shortly afterwards, Zhu [32] succeeded in verifying two special cases and constructing a counterexample in general.

The first objective of the present article is to investigate the integrality of A over A^H more thoroughly (here A^H stands for the invariants of the given coaction). A part of the argument given in [7,24] for commutative H carries over without problems. Since A is commutative, $A \otimes H$ can be regarded as an A-algebra with respect to the action on the first tensorand. Since $A \otimes H$ is free of finite rank over A, with each element $u \in A \otimes H$ one can associate its characteristic polynomial $P_{A\otimes H/A}(u,t) \in A[t]$. Letting

$$P_{A\otimes H/A}(\delta a, t) = \sum_{i=0}^{n} c_i t^i$$

for $a \in A$, where $n = \dim H$, one has $c_n = 1$ and $\sum_{i=0}^{n} c_i a^i = 0$. If H is commutative then $c_0, \ldots, c_n \in A^H$, and the desired integrality is achieved. At this point the noncommutativity of H spoils the game altogether. It is nevertheless shown in Theorem 2.5 that $c_0, \ldots, c_n \in A^H$ for any H provided that A is H-reduced, that is, A has no nonzero H-costable nil ideals. Crucial for the proof is the freeness of finite-dimensional Hopf algebras over commutative right coideal subalgebras. Because of nice functorial properties of characteristic polynomials, it is possible to pass to finite-dimensional Hopf algebras $E \otimes H$ over various fields E where the characteristic polynomials can be computed using the above-mentioned freeness.

The integrality of A over A^H is proved in Proposition 2.7 and Theorem 6.2 not only for an H-reduced A but also in other situations. It always holds when either $\operatorname{char} K \neq 0$, or H is cosemisimple, or there exists a total integral $H \to A$ in the sense of Doi [9]. In Zhu's paper [32, Theorem 2.1, Corollary 3.3] the integrality was proved under the assumptions that either $\operatorname{char} K$ does not divide $\dim H$ and H is involutory or $\operatorname{char} K \neq 0$ and H^* has a cocommutative coradical. In the first of these two results H is necessarily semisimple and cosemisimple. At the same time it is still not known if every semisimple Hopf algebra is involutory when $\operatorname{char} K \neq 0$ [19].

The invariance of characteristic polynomials enables one to investigate the map $\operatorname{Spec} A \to \operatorname{Spec} A^H$ between the prime spectra of rings A and A^H much in the same spirit as was done in case of commutative H. It is shown in Theorem 3.3 that this map has finite fibers, is open and satisfies the going-down property.

With each $\mathfrak{p} \in \operatorname{Spec} A$ we associate the orbital subalgebra $O(\mathfrak{p}) \subset k(\mathfrak{p}) \otimes H$ and the stabilizer subalgebra $\operatorname{St}(\mathfrak{p}) \subset k(\mathfrak{p}) \otimes H^*$ where $k(\mathfrak{p})$ denotes the residue field of the local ring $A_{\mathfrak{p}}$. A prime $\mathfrak{p}$ will be called H-regular if $\dim_{k(\mathfrak{p})} O(\mathfrak{p})$ does not change in a suitable neighborhood of $\mathfrak{p}$ in $\operatorname{Spec} A$. The assumption that the algebra A is H-reduced and all prime ideals of A are H-regular implies that A is a finitely generated projective A^H-module and the H-costable ideals of A correspond bijectively to the ideals of A^H. This is the content of Theorem 4.3 which extends my earlier work [28]. The conclusions of this theorem were known to be true when A is an H-Galois extension of A^H.

The purpose of Section 5 is to show the existence of a total integral $H \to A$ for an H-comodule algebra with semisimple stabilizer subalgebras $\mathrm{St}(\mathfrak{p})$. This is one of cases in which the canonical maps $A^H \to (A/I)^H$ are surjective for all H-costable ideals I of A. In general, if the latter property is fulfilled, A will be called weakly reductive with respect to coaction of H. This property is essential in the final major result of this paper. Theorem 6.2 states that A^H is Cohen–Macaulay whenever A is Cohen–Macaulay and weakly reductive. This generalizes a result of Hochster and Eagon [16, Proposition 13] according to which the Cohen–Macaulay property of a commutative ring A descends to the subring of invariants of a finite group G acting on A by automorphisms provided that the order of G is invertible in A. A point of interest here is that an H-reduced A is always weakly reductive when $\mathrm{char}\, K = 0$, even if H is not cosemisimple. Theorem 6.2 also gives sufficient conditions for A to be a finitely generated A^H-module.

Summarizing, the invariants of a noncommutative H behave as decently as in the commutative case provided that one is going to be content with the H-reduced algebras A. The assumption that K is a field was made in this introduction only to illustrate the results in the simplest case. Working over a commutative base ring involves no significant complications.

1. Preliminaries

We fix a few notations for the whole paper. Assume that K is a commutative ring, H is a Hopf algebra over K whose underlying K-module is finitely generated and projective, and A is a commutative right H-comodule algebra. We will consider mainly right comodules, and the prefix "right" will be omitted. All tensor products, when the base ring is not indicated, are taken over K. The comultiplication, counit and antipode in H are denoted as Δ, ε and σ, respectively. We write symbolically $\Delta h = \sum_{(h)} h' \otimes h''$ and $(\Delta \otimes \mathrm{id})\Delta h = \sum_{(h)} h' \otimes h'' \otimes h'''$ for $h \in H$.

For every H-comodule M denote by $\delta : M \to M \otimes H$ the corresponding structure map. In particular, $\delta : A \to A \otimes H$ is a homomorphism of unital algebras. Denote by $M^H \subset M$ the K-submodule of invariants. Thus $M^H = \{v \in M \mid \delta v = v \otimes 1\}$. Clearly A^H is a subalgebra of A. Next, $\mathscr{M}_A^H$ stands for the category of right (H, A)-Hopf modules [9]. The objects of $\mathscr{M}_A^H$ are right A-modules equipped with a right H-comodule structure such that

$$\delta(va) = \delta(v)\delta(a) \quad \text{for all } v \in M \text{ and } a \in A. \tag{1.1}$$

Here and later we regard $M \otimes H$ as a right $A \otimes H$-module by means of the operation $(v \otimes g)(a \otimes h) = va \otimes gh$ for $v \in M$, $a \in A$ and $g, h \in H$. The morphisms in $\mathscr{M}_A^H$ are maps which are compatible with both structures.

Lemma 1.1. *Suppose that $S \subset A^H$ is any multiplicatively closed subset. Then $S^{-1}A$ is an H-comodule algebra and $S^{-1}M \in \mathcal{M}^H_{S^{-1}A}$ for every $M \in \mathcal{M}^H_A$. Moreover, one has $(S^{-1}M)^H \cong S^{-1}(M^H)$.*

Proof. Let us regard $M \otimes H$ as an A^H-module by means of the action on the first tensorand. The two maps $\delta, \imath : M \to M \otimes H$ where $\imath(v) = v \otimes 1$ for $v \in M$ are homomorphisms of A^H-modules. Hence δ extends to a map $S^{-1}M \to S^{-1}M \otimes H$ which makes $S^{-1}M$ into an H-comodule. One checks easily that (1.1) is fulfilled for the action of $S^{-1}A$ on $S^{-1}M$. The assertion about $(S^{-1}M)^H$ is obtained by applying the localization functor $S^{-1}(?)$ to the exact sequence of A^H-modules

$$0 \to M^H \to M \xrightarrow{\delta - \imath} M \otimes H. \qquad \square$$

This lemma will be used in two cases. If $S = \{s^i \mid i \geqslant 0\}$ where $s \in A^H$ then the localizations are denoted as A_s and M_s. If $S = A^H \backslash \mathfrak{q}$ where $\mathfrak{q} \in \operatorname{Spec} A^H$ then the notations are $A_{\mathfrak{q}}$ and $M_{\mathfrak{q}}$.

An ideal I of A is called H-*costable* if $\delta(I) \subset I \otimes H$. This makes sense since $I \otimes H$ is embedded into $A \otimes H$ by the K-projectivity of H. If I is H-costable then $\delta : A \to A \otimes H$ induces a ring homomorphism $A/I \to A/I \otimes H$ which makes A/I into an H-comodule algebra.

If $\mathfrak{q} \in \operatorname{Spec} K$ then $H_{\mathfrak{q}} = K_{\mathfrak{q}} \otimes H$ is a free module over the local ring $K_{\mathfrak{q}}$. Denote by $\operatorname{rk}_{\mathfrak{q}} H$ its rank. If $\operatorname{rk}_{\mathfrak{q}} H$ does not depend on $\mathfrak{q}$, then H is K-projective of *constant rank*.

Lemma 1.2. *One has $K \cong \prod K_i$, $H \cong \prod H_i$, $A \cong \prod A_i$, where the products are taken over a finite set of indices, each K_i is a commutative ring, H_i is a Hopf algebra over K_i which is K_i-projective of constant rank, and A_i is an H_i-comodule algebra. Moreover, $A^H \cong \prod A_i^{H_i}$.*

Proof. For each $i > 0$ the subset $X_i = \{\mathfrak{q} \in \operatorname{Spec} K \mid \operatorname{rk}_{\mathfrak{q}} H = i\}$ is open in $\operatorname{Spec} K$ [4, Chapter II, Section 5, Theorem 1]. Now $\operatorname{Spec} K$ is a finite disjoint union of these subsets X_i, where we remove the empty subsets. By Bourbaki [4, Chapter II, Section 4, Proposition 15] K contains a family of orthogonal idempotents $\{e_i\}$ such that $\sum e_i = 1$ and $X_i = \{\mathfrak{q} \in \operatorname{Spec} K \mid 1 - e_i \in \mathfrak{q}\}$ for each i. If V is any K-module then $V \cong \prod V_i$, where $V_i = V/(1 - e_i)V$. This gives the first three isomorphisms of the lemma. Similarly, $A \otimes H \cong \prod (A_i \otimes H_i)$ and the map $\delta : A \to A \otimes H$ is compatible with the cartesian products. Hence the assertion about A^H. $\square$

As is well known, the dual $H^* = \operatorname{Hom}_K(H, K)$ of H is a Hopf algebra in a natural way. The H-comodule structures are in a bijective correspondence with the left H^*-module structures [26, Proposition 1]. The operator giving the action of $\xi \in H^*$ on an H-comodule M can be written as the composite

$$L_\xi : M \xrightarrow{\delta} M \otimes H \xrightarrow{\mathrm{id} \otimes \xi} M \otimes K \cong M. \tag{1.2}$$

One sees that $M^H = \{v \in M \mid (H^*)^+ v = 0\}$ where $(H^*)^+ = \{\xi \in H^* \mid \xi(1) = 0\}$. We may regard H as a right H-comodule via Δ.

Lemma 1.3. *H is a finitely generated projective H^*-module with respect to the corresponding action of H^*.*

Proof. By Pareigis [26, Propositions 2, 3, Lemma 2] with H and H^* interchanged the set of left integrals $P(H) = \{x \in H \mid hx = \varepsilon(h)x \text{ for all } h \in H\}$ is a rank one projective K-module and the map $H^* \otimes P(H) \to H$ defined by the rule $\xi \otimes x \mapsto L_\xi(x)$ is bijective. Clearly $H^* \otimes P(H)$ is a finitely projective H^*-module. □

A reduction of the base ring to a field is one of our tools. We will need several facts from earlier work. Assume until the end of this section that *K is a field* and *H is a finite-dimensional Hopf algebra*. A *left* (respectively, *right*) *coideal subalgebra* $B \subset H$ is a subalgebra satisfying $\Delta(B) \subset H \otimes B$ (respectively, $\Delta(B) \subset B \otimes H$). If H is cocommutative then the two inclusions are equivalent to one another, and so every left coideal subalgebra of H is a Hopf subalgebra. The next result is due to Masuoka [20, (2.1)]:

Proposition 1.4. *Suppose that $B \subset H$ is a right coideal subalgebra. Then B is Frobenius if and only if H is left and right B-free.*

Proposition 1.5. *Every commutative right coideal subalgebra $B \subset H$ is Frobenius, and so H is a free B-module from either side.*

This is contained in Koppinen's paper [17, Corollary 2.5] where the result is attributed to the referee.

Proposition 1.6. *Suppose that $B \subset H$ is a Frobenius right coideal subalgebra and $B^+ = \{b \in B \mid \varepsilon(b) = 0\}$. Then*:

(i) *$C = (H/HB^+)^*$ is a Frobenius left coideal subalgebra of H^**;
(ii) *$B \cong (H^*/C^+H^*)^*$ where $C^+ = \{\xi \in C \mid \xi(1) = 0\}$*;
(iii) *the category $\mathscr{M}_B^H$ is equivalent to the category of C-modules.*

This is a version of Masuoka's result [20, (2.10)] where a similar relationship between the right coideal subalgebras in both H and H^* is described. One connects the two formulations by taking the opposite multiplications in A and H and applying [20, (1.1), (1.2)].

2. Characteristic polynomials and integrality over invariants

Suppose that A is any commutative ring and U is an associative A-algebra such that U is projective of constant rank n as an A-module. In this case one can define the *norm* $N_{U/A}(u)\in A$ for every $u\in U$ [3, Chapter III, Section 9]; [4, Chapter II, Section 5, Exercise 9]. In fact, if U has a basis $e_1,\dots,e_n$ over A, then $ue_j=\sum_{i=1}^n a_{ij}e_i$ with coefficients in A, and $N_{U/A}(u)$ is the determinant of the square matrix with entries a_{ij}, $1\leqslant i,j\leqslant n$. In general, one can pass to localizations U_s and A_s with respect to multiplicatively closed subsets $\{s^i\mid i\geqslant 0\}$ where $s\in A$. There exist a finite number of elements $s_1,\dots,s_m\in A$ which generate the whole A as an ideal and such that U_{s_i} is free of rank n over A_{s_i} for each $i=1,\dots,m$. If u_i denotes the image of u in U_{s_i}, then $N_{U_{s_i}/A_{s_i}}(u_i)\in A_{s_i}$ is defined, and any two of these norms corresponding to a pair of indices i,j have the same image in $A_{s_is_j}$. Then this collection of elements in localizations can be glued to an element $N_{U/A}(u)\in A$ using the well-known exact sequence

$$0\to A\to\prod_i A_{s_i}\rightrightarrows\prod_{i,j}A_{s_is_j}.$$

The *characteristic polynomial* of u is obtained by adjoining an indeterminate t as

$$P_{U/A}(u,t)=N_{U[t]/A[t]}(t-u)\in A[t].$$

In particular, $(-1)^nN_{U/A}(u)$ is the coefficient of t^0 in $P_{U/A}(u,t)$. The well-known properties of the characteristic polynomials and the norm are listed below:

(P1) $P_{U/A}(u,u)=0$ (the substitution of u for t).
(P2) $P_{V/A}(\varphi u,t)=P_{U/A}(u,t)$ when $\varphi:U\to V$ is an isomorphism of A-algebras.
(P3) $P_{B\otimes_AU/B}(1\otimes u,t)=\gamma^tP_{U/A}(u,t)$ where $\gamma:A\to B$ is a homomorphism of commutative rings and $\gamma^t:A[t]\to B[t]$ is its extension such that $t\mapsto t$.
(P4) If $V\subset U$ is an A-subalgebra such that V is projective as an A-module and U is free, say of rank r, as a left V-module, then $P_{U/A}(u,t)=P_{V/A}(u,t)^r$ for every $u\in V$.
(P5) If $a\in A$ then $P_{U/A}(a,t)=(t-a)^n$.
(P6) If A is a field and $\dim_AU=n$, then the equality $P_{U/A}(u,t)=t^n$ is a necessary and sufficient condition for $u\in U$ to be nilpotent.
(P7) An element u is invertible in U if and only if $N_{U/A}(u)$ is invertible in A.

Suppose further that A is a commutative H-comodule algebra as was specified in Section 1. Given a ring homomorphism $\alpha:A\to E$ into a field E, define

$$A_\alpha=(E\otimes 1)\cdot\delta_\alpha(A)\subset E\otimes H,\tag{2.1}$$

where δ_α is the composite

$$A \xrightarrow{\delta} A \otimes H \xrightarrow{\alpha\otimes\mathrm{id}} E \otimes H. \tag{2.2}$$

Lemma 2.1. *A_α is a right coideal subalgebra of the Hopf algebra $E \otimes H$ over E. If Δ_E denotes the map* $\mathrm{id} \otimes \Delta : E \otimes H \to E \otimes H \otimes H$, *then*

$$(\delta_\alpha \otimes \mathrm{id}) \circ \delta = \Delta_E \circ \delta_\alpha. \tag{2.3}$$

Proof. Since δ is a ring homomorphism, so too is δ_α, whence A_α is a subalgebra of $E \otimes H$. Formula (2.3) is seen from the commutative diagram

$$\begin{array}{ccccc}
A & \xrightarrow{\quad\delta\quad} & A \otimes H & \xrightarrow{\quad\alpha\otimes\mathrm{id}\quad} & E \otimes H \\
\downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\mathrm{id}\otimes\Delta} & & \downarrow{\scriptstyle\mathrm{id}\otimes\Delta} \\
A \otimes H & \xrightarrow{\delta\otimes\mathrm{id}} & A \otimes H \otimes H & \xrightarrow{\alpha\otimes\mathrm{id}\otimes\mathrm{id}} & E \otimes H \otimes H.
\end{array}$$

It follows from (2.3) that $\Delta_E(A_\alpha) \subset A_\alpha \otimes H$. Under the canonical identification $(E \otimes H) \otimes_E (E \otimes H) \cong E \otimes H \otimes H$, the comultiplication in $E \otimes H$ is precisely Δ_E. Hence A_α is a right coideal. $\square$

Remark. One can also view $E \otimes H$ as an H-comodule algebra with respect to Δ_E and A_α as its H-comodule subalgebra. Formula (2.3) says that $\delta_\alpha : A \to E \otimes H$ is a homomorphism of H-comodule algebras.

Lemma 2.2. *Suppose that $B \subset C$ is an extension of commutative rings such that B is Artinian and C is B-projective. If M is a C-module such that M is B-projective and $M/\mathfrak{n}M$ is free of rank r over $C/\mathfrak{n}C$ for every maximal ideal $\mathfrak{n}$ of B where r does not depend on $\mathfrak{n}$, then M is free of rank r over C.*

Proof. Let J be the Jacobson radical of B. Then $B/J \cong \prod B/\mathfrak{n}$, the product over the finitely many maximal ideals of B. Furthermore, $C/JC \cong \prod C/\mathfrak{n}C$ and $M/JM \cong \prod M/\mathfrak{n}M$ [4, Chapter II, Section 1, Proposition 6]. It follows from the hypotheses of the lemma that M/JM is a free C/JC-module of rank r. Let F be a free C-module of rank r. There exists then a homomorphism of C-modules $\varphi : F \to M$ which induces an isomorphism $F/JF \cong M/JM$. Since J is a nilpotent ideal of B, we conclude that φ is surjective [4, Chapter II, Section 3, Corollary 1 to Proposition 4]. Put $N = \ker \varphi$. By the B-projectivity of M the exactness of sequence $0 \to N \to F \to M \to 0$ is preserved when passing to reductions modulo J. Hence $N/JN = 0$, and $N = 0$ by Nakayama's Lemma. Thus φ is an isomorphism. $\square$

The ring $A \otimes H$ contains $A \otimes 1$ in its center. Hence we may view $A \otimes H$ as an A-algebra using the canonical homomorphism $A \to A \otimes 1$. Since H is finitely projective K-module, so too is $A \otimes H$ as an A-module. If H is a projective K-module of rank n, the A-module $A\otimes H$ has rank n as well. In this case the characteristic polynomial $P_{A\otimes H/A}(u,t)\in A[t]$ is defined for every $u\in A\otimes H$.

Proposition 2.3. *Suppose that K is a field. If $b\in B$ where B is a commutative right coideal subalgebra of H, then $P_{B\otimes H/B}(\Delta b,t) = P_{H/K}(b,t)$.*

The conclusion of this proposition means, in particular, that the first polynomial has all coefficients in $K\subset B$.

Proof. We regard $B\otimes H$ as a B-algebra in accordance with the previous explanation. By Proposition 1.5 H is free over B with respect to the action by left multiplications. Let $r = \mathrm{rk}_B\, H$. Put $C = (B\otimes 1)\cdot \Delta(B)\subset B\otimes H$. Since $\Delta : B\to B\otimes H$ is a ring homomorphism, C is a commutative B-subalgebra of $B\otimes H$. We will prove first that $B\otimes H$ is a free C-module of rank r with respect to the action by left multiplications.

Define $\Phi : B\otimes B\to B\otimes H$ by $\Phi(a\otimes b) = (a\otimes 1)\cdot \Delta b$ for $a,b\in B$. Then Φ is a ring homomorphism and $\mathrm{Im}\,\Phi = C$. Since B is commutative and H is a free B-module of finite rank, B is a B-module direct summand of H [4, Chapter II, Section 5, Exercise 4]. Let $\psi : H\to B$ be a retraction, so that $\psi(1) = 1$ and $\psi(bh) = b\psi(h)$ for all $b\in B$ and $h\in H$. Define $\Psi : B\otimes H\to B\otimes B$ by $\Psi(a\otimes h) = \sum_{(h)} a\psi(\sigma h')\otimes h''$. Then

$$\Psi(\Delta b) = \sum_{(b)} b'\psi(\sigma b'')\otimes b''' = \sum_{(b)} \psi(b'\cdot \sigma b'')\otimes b''' = \sum_{(b)} \varepsilon(b')\psi(1)\otimes b'' = 1\otimes b$$

for $b\in B$. This shows that $\Psi\circ\Phi = \mathrm{id}$. In particular, Φ is a ring isomorphism of $B\otimes B$ onto C. We have also $B\otimes H = C\oplus \ker\Psi$. Both Φ and Ψ are B-linear with respect to the actions of B on the first tensorands. Then C is a B-module direct summand of $B\otimes H$. Let $\mathfrak{n}$ be a maximal ideal of B and $E = B/\mathfrak{n}$ its residue field. The embedding of C into $B\otimes H$ induces an injective homomorphism of E-algebras

$$C/\mathfrak{n}C\to (B\otimes H)/\mathfrak{n}(B\otimes H)\cong E\otimes H.$$

The image of the latter coincides with B_β where $\beta : B\to E$ is the canonical projection and B_β is defined as in (2.1). By Lemma 2.1 B_β is a right coideal subalgebra of $E\otimes H$, and by Proposition 1.5 $E\otimes H$ is free over B_β. Now the reduction of Φ modulo $\mathfrak{n}$ gives an E-linear bijection $E\otimes B\cong C/\mathfrak{n}C\cong B_\beta$. Hence $\dim_E B_\beta = \dim_K B$, and so

$$\mathrm{rk}_{B_\beta}\, E\otimes H = \dim_E(E\otimes H)/\dim_E B_\beta = \dim_K H/\dim_K B = r.$$

We see that the hypotheses of Lemma 2.2 are fulfilled for $M = B\otimes H$, yielding the desired freeness.

Let $b\in B$, and so $\Delta b\in C$. Applying successively (P4), (P2), (P3), and (P4) again, we find

$$\begin{aligned} P_{B\otimes H/B}(\Delta b,t) &= P_{C/B}(\Delta b,t)^r = P_{B\otimes B/B\otimes 1}(1\otimes b,t)^r \\ &= P_{B/K}(b,t)^r = P_{H/K}(b,t). \qquad \square \end{aligned}$$

Lemma 2.4. *Suppose that $\alpha : A \to E$ is a ring homomorphism into a field E. If $b = \delta_\alpha(a)$ where $a \in A$, then*

$$P_{A_\alpha \otimes H/A_\alpha}(\Delta_E b, t) = P_{E \otimes H/E}(b, t). \tag{2.4}$$

Proof. Apply Proposition 2.3 to the Hopf algebra $E \otimes H$ over the field E and its right coideal subalgebra $B = A_\alpha$ (see Lemma 2.1). □

When H is K-projective of constant rank, we say that A has *invariant characteristic polynomials* if $P_{A \otimes H/A}(\delta a, t)$ has all coefficients in A^H for every $a \in A$. When the rank of H is not constant, we say that A has invariant characteristic polynomials if so do the H_i-comodule algebras A_i in the cartesian product decomposition of Lemma 1.2. In case of a commutative H the invariance of characteristic polynomials for any A was proved in [7, Chapter III, Section 12]; [24, Chapter III, Section 2]. If H is not commutative, additional assumptions are needed. The largest H-costable nil ideal of A will be called the H-*radical* of A. We say that A is H-*reduced* if its H-radical is equal to (0).

Theorem 2.5. *If A is H-reduced or, more generally, if there exists a homomorphism of commutative H-comodule algebras $\varphi : A' \to A$ such that A' is H-reduced and $A = \varphi(A')A^H$ then A has invariant characteristic polynomials.*

Proof. Consider first the case where A is H-reduced. The H_i-comodule algebras A_i in Lemma 1.2 are then H_i-reduced too. So we may assume without loss of generality that H is K-projective of constant rank.

Suppose that $\alpha : A \to E$ is a ring homomorphism into a field E. Define δ_α as in (2.2), and let $\lambda_\alpha = \imath \circ \alpha$ where $\imath : E \to E \otimes H$ is given by $c \mapsto c \otimes 1$. Both δ_α and λ_α take values in A_α. We first prove that

$$\delta_\alpha^t P_{A \otimes H/A}(\delta a, t) = \lambda_\alpha^t P_{A \otimes H/A}(\delta a, t) \quad \text{in } A_\alpha[t]. \tag{2.5}$$

If $\gamma : A \to A_\alpha$ is any ring homomorphism then

$$\gamma^t P_{A \otimes H/A}(\delta a, t) = P_{A_\alpha \otimes H/A_\alpha}((\gamma \otimes \mathrm{id})\delta a, t)$$

by (P3) since $A_\alpha \otimes_A (A \otimes H) \cong A_\alpha \otimes H$ and the element $1 \otimes u$, where $u \in A \otimes H$, corresponds under this isomorphism to $(\gamma \otimes \mathrm{id})u \in A_\alpha \otimes H$. In case $\gamma = \delta_\alpha$, denoting $b = \delta_\alpha(a)$ and using (2.3), (2.4), we obtain

$$\delta_\alpha^t P_{A \otimes H/A}(\delta a, t) = P_{A_\alpha \otimes H/A_\alpha}(\Delta_E b, t) = P_{E \otimes H/E}(b, t).$$

In case $\gamma = \lambda_\alpha$ we have $(\gamma \otimes \mathrm{id}) \circ \delta = (\imath \otimes \mathrm{id}) \circ \delta_\alpha$, whence $(\gamma \otimes \mathrm{id})\delta a = (\imath \otimes \mathrm{id})b$. An application of (P3) for the ring homomorphism $\imath : E \to A_\alpha$ yields

$$\lambda_\alpha^t P_{A \otimes H/A}(\delta a, t) = P_{A_\alpha \otimes H/A_\alpha}((\imath \otimes \mathrm{id})b, t) = P_{E \otimes H/E}(b, t).$$

Thus (2.5) is proved. Let $P_{A\otimes H/A}(\delta a, t) = \sum_{i=0}^{n} c_i t^i$ with $c_0, \dots, c_n \in A$. If $\mathfrak{p} = \ker \alpha$ then the sequence

$$0 \to \mathfrak{p} \otimes H \to A \otimes H \xrightarrow{\alpha \otimes \mathrm{id}} E \otimes H$$

is exact by K-projectivity of H. Formula (2.5) means that $\delta_\alpha(c_i) = \lambda_\alpha(c_i)$, whence $\delta c_i - c_i \otimes 1 \in \ker(\alpha \otimes \mathrm{id}) = \mathfrak{p} \otimes H$ for each i. This can be rewritten in terms of the H^*-module structure on A as $\xi c_i - \xi(1) c_i \in \mathfrak{p}$ for all $\xi \in H^*$, or $(H^*)^+ c_i \subset \mathfrak{p}$. These inclusions hold for every $\mathfrak{p} \in \operatorname{Spec} A$ since any prime ideal $\mathfrak{p}$ is the kernel of a homomorphism into a field. Put $J = AV$ where $V = \sum_{i=0}^{n} (H^*)^+ c_i$. By the above J is contained in the nil radical of A. Since $(H^*)^+$ is an ideal of H^*, it is clear that V is an H^*-submodule of A, whence so too is J. In other words, J is an H-costable nil ideal of A. It follows that $J = 0$ by the assumption on A. Thus $(H^*)^+ c_i = 0$, and so $c_i \in A^H$.

If I is an H-costable ideal of A and $\pi : A \to \bar{A} = A/I$ is the canonical projection then $\delta \circ \pi = (\pi \otimes \mathrm{id}) \circ \delta$, and so $P_{\bar{A}\otimes H/\bar{A}}(\delta \pi a, t) = \pi^t P_{A\otimes H/A}(\delta a, t)$ for every $a \in A$ by (P3). This polynomial has all coefficients in $\pi(A^H) \subset (A/I)^H$. Thus A/I has invariant characteristic polynomials.

Consider now the general case of Theorem 2.5. Suppose that φ is given. If φ is surjective, then we are done by the previous step. Otherwise consider the polynomial algebra $A'' = A'[X]$ where X is any set of indeterminates. Extend $\delta : A' \to A' \otimes H$ to a ring homomorphism $A'' \to A'' \otimes H$ setting $\delta(x) = x \otimes 1$ for all $x \in X$. This makes A'' into an H-comodule commutative algebra. Denote by R the H-radical of A''. Each $f \in R$ is nilpotent, whence all coefficients of f are nilpotent [3, Chapter IV, Section 1, Proposition 9]. For every monomial y in x's denote by $R_y \subset A'$ the subset consisting of all elements occurring as a coefficient of y in some $f \in R$. Clearly R_y is a nil ideal of A'. Since R is H-costable, so too is R_y. It follows that $R_y = 0$ since A' is H-reduced. As this holds for every monomial y, we conclude that $R = 0$. Thus A'' is H-reduced. We can extend φ to a homomorphism of H-comodule algebras $\psi : A'' \to A$ sending each $x \in X$ to an arbitrary element of A^H. Taking the set X big enough, we can thus obtain a surjective homomorphism ψ. As has been pointed out already, this suffices to complete the proof. $\square$

Proposition 2.6. *Suppose that A has invariant characteristic polynomials and m is a positive integer such that $\mathrm{rk}_{\mathfrak{q}} H$ divides m for every $\mathfrak{q} \in \operatorname{Spec} K$. If $\bar{a} \in (A/I)^H$ where I is an H-costable ideal of A then $\binom{m}{j} \bar{a}^j$ belongs to the image of the canonical map $A^H \to (A/I)^H$ for every $j = 0, \dots, m$.*

Proof. Lemma 1.2 gives decompositions $A^H \cong \prod A_i^{H_i}$ and $(A/I)^H \cong \prod (A_i/I_i)^{H_i}$ where each I_i is an H_i-costable ideal of A_i. The assumption on m means that m is divisible by the ranks of the projective K_i-modules H_i for all i occurring here. So it suffices to prove the assertion of the proposition for the canonical maps

$A_i^{H_i} \to (A_i/I_i)^{H_i}$. We may assume therefore that H has constant rank n and $m = dn$ for some integer $d > 0$.

Let $\pi : A \to \bar{A} = A/I$ denote the canonical projection, and let $a \in A$ be any representative of $\bar{a}$. By (P3) and (P5)

$$\pi^t P_{A\otimes H/A}(\delta a, t) = P_{\bar{A}\otimes H/\bar{A}}(\delta \bar{a}, t) = P_{\bar{A}\otimes H/\bar{A}}(\bar{a} \otimes 1, t) = (t - \bar{a})^n.$$

Thus $\binom{n}{l}(-\bar{a})^l = \pi(c_{n-l})$ for $l = 0, \ldots, n$ where $\sum_{l=0}^n c_l t^l = P_{A\otimes H/A}(\delta a, t)$. By the hypothesis $c_0, \ldots, c_n \in A^H$. Now

$$\sum_{j=0}^m \binom{m}{j} \bar{a}^j t^{m-j} = (t + \bar{a})^m = (t + \bar{a})^{dn} = \left(\sum_{l=0}^n \binom{n}{l} \bar{a}^l t^{n-l} \right)^d,$$

and therefore the elements $\binom{m}{j}\bar{a}^j$ with $j = 0, \ldots, m$ belong to the subalgebra of A/I generated by the images of $c_0, \ldots, c_n$. $\square$

Remark. In particular, $\bar{a}^m$ is in the image of $A^H \to (A/I)^H$ for every $\bar{a} \in (A/I)^H$. This can be regarded as a *geometric reductivity* of finite Hopf algebras. Classically, the geometric reductivity is a property of a reductive algebraic group G over a field of characteristic $p > 0$ which serves as a substitute for linear reductivity [14,23]. One of its formulations is as follows: if G operates rationally on a commutative algebra A as a group of automorphisms and I is a G-stable ideal of A, then for every G-invariant $\bar{a} \in (A/I)^G$ there exists an integer $m > 0$ such that $\bar{a}^m$ has a representative in A^G. The geometric reductivity of finite group schemes is a byproduct of the norm [31].

Proposition 2.7. *A is integral over A^H in any of the following two cases*:

(a) *A has invariant characteristic polynomials*,
(b) *the H-radical R of A is $\mathbb{Z}$-torsion.*

Proof. (a) It suffices to show that each A_i in Lemma 1.2 is integral over $A_i^{H_i}$ by [4, Chapter V, Section 1, Proposition 3]. So we may assume, without loss of generality, that H is K-projective of constant rank n. Given $a \in A$, let $P_{A\otimes H/A}(\delta a, t) = \sum_{i=0}^n c_i t^i$. By the hypothesis $c_0, \ldots, c_n \in A^H$. Property (P1) ensures that $\sum_{i=0}^n (c_i \otimes 1)(\delta a)^i = 0$ in $A \otimes H$. Applying the ring homomorphism $\mathrm{id} \otimes \varepsilon : A \otimes H \to A$ to both sides of this equality, we get $\sum_{i=0}^n c_i a^i = 0$ since $(\mathrm{id} \otimes \varepsilon) \circ \delta = \mathrm{id}$. Here $c_n = 1$, and so a is integral over A^H.

(b) The H-comodule algebra A/R is H-reduced, and so A/R has invariant characteristic polynomials by Theorem 2.5. Thus A/R is integral over $(A/R)^H$ by case (a). Let $B \subset A$ denote the preimage of $(A/R)^H$ with respect to the canonical map $A \to A/R$. Clearly, B is a subalgebra of A containing A^H and A is integral over B. It remains to prove that B is integral over A^H [4, Chapter V, Section 1, Proposition 6].

Let $b \in B$. In view of the exact sequence

$$R \otimes H \to A \otimes H \to (A/R) \otimes H \to 0$$

the element $\delta b - b \otimes 1 \in A \otimes H$ which goes to 0 in $(A/R) \otimes H$ belongs to the image of $R \otimes H$. Thus $\delta b = b \otimes 1 + x$ where $x = x_1 \otimes h_1 + \cdots + x_l \otimes h_l$ with $x_1, \ldots, x_l \in R$ and $h_1, \ldots, h_l \in H$. Since R is a nil ideal, the ideal of A generated by finitely many $x_1, \ldots, x_l$ is nilpotent. There exists therefore an integer $n > 0$ such that $x^n = 0$. By the hypothesis there exists an integer $e > 0$ such that $ex_j = 0$ for all j, hence also $ex = 0$. Take an integer $m > 0$ such that e divides all binomial coefficients $\binom{m}{i}$ for $i = 1, \ldots, n$ (for instance, $m = e \cdot n!$ will do). Noting that $b \otimes 1$ is central in the algebra $A \otimes H$, we obtain $\delta(b^m) = (\delta b)^m = \sum_{i=0}^m \binom{m}{i}(b^{m-i} \otimes 1)x^i = b^m \otimes 1$. This shows that $b^m \in A^H$. Hence b is integral over the subring A^H. $\square$

Remark. If A is an algebra over a field of characteristic $p > 0$ then condition (b) is fulfilled since $pA = 0$.

3. The orbital subalgebras and the quotient map

For each $\mathfrak{p} \in \operatorname{Spec} A$ denote by $k(\mathfrak{p})$ the residue field of the local ring $A_\mathfrak{p}$. The same notation will be used for commutative rings other than A. Let $\alpha_\mathfrak{p} : A \to k(\mathfrak{p})$ be the canonical ring homomorphism. Denote by $O(\mathfrak{p})$ the commutative right coideal subalgebra $A_{\alpha_\mathfrak{p}}$ of the Hopf algebra $k(\mathfrak{p}) \otimes H$ over $k(\mathfrak{p})$ defined in (2.1). We call $O(\mathfrak{p})$ the *orbital subalgebra* associated with $\mathfrak{p}$. In geometric terms $\operatorname{Spec} O(\mathfrak{p})$ is isomorphic with a closed subscheme of $\operatorname{Spec} k(\mathfrak{p}) \times_{\operatorname{Spec} K} \operatorname{Spec} A$; when H is commutative and $G = \operatorname{Spec} H$, this subscheme is called the G-orbit of $\mathfrak{p}$. Let $\delta_\mathfrak{p} = \delta_{\alpha_\mathfrak{p}}$ as in (2.2). Thus $\delta_\mathfrak{p}$ is a ring homomorphism $A \to k(\mathfrak{p}) \otimes H$ and $O(\mathfrak{p}) = (k(\mathfrak{p}) \otimes 1) \cdot \delta_\mathfrak{p}(A)$.

Lemma 3.1. *The kernel of $\delta_\mathfrak{p}$ is the largest H-costable ideal of A contained in $\mathfrak{p}$.*

Proof. In view of Lemma 2.1 $\delta_\mathfrak{p}$ is a homomorphism of H-comodule algebras. Hence $\ker \delta_\mathfrak{p}$ is an H-costable ideal of A. The composite of two arrows at the top of commutative diagram

$$\begin{tikzcd} A \arrow[r, "\delta"] \arrow[dr, "\mathrm{id}"'] & A \otimes H \arrow[r, "\alpha_\mathfrak{p} \otimes \mathrm{id}"] \arrow[d, "\mathrm{id} \otimes \varepsilon"] & k(\mathfrak{p}) \otimes H \arrow[d, "\mathrm{id} \otimes \varepsilon"] \\ & A \arrow[r, "\alpha_\mathfrak{p}"] & k(\mathfrak{p}) \end{tikzcd} \tag{3.1}$$

equals $\delta_\mathfrak{p}$, whence $(\mathrm{id} \otimes \varepsilon) \circ \delta_\mathfrak{p} = \alpha_\mathfrak{p}$. This yields $\ker \delta_\mathfrak{p} \subset \ker \alpha_\mathfrak{p} = \mathfrak{p}$. If I is any H-costable ideal of A and $I \subset \mathfrak{p}$, then $\delta_\mathfrak{p}(I) \subset (\alpha_\mathfrak{p} \otimes \mathrm{id})(I \otimes H) = 0$. $\square$

Lemma 3.2. *Let $\gamma : A \to B$ be a homomorphism of commutative H-comodule algebras, and let $\mathfrak{p} = \gamma^{-1}(\mathfrak{q})$ where $\mathfrak{q} \in \operatorname{Spec} B$. Then*:

(i) $(\bar{\gamma} \otimes \mathrm{id}) \circ \delta_{\mathfrak{p}} = \delta_{\mathfrak{q}} \circ \gamma$ *where* $\bar{\gamma} : k(\mathfrak{p}) \to k(\mathfrak{q})$ *is induced by* γ.
(ii) $k(\mathfrak{q}) \otimes_{k(\mathfrak{p})} O(\mathfrak{p})$ *is canonically embedded into* $O(\mathfrak{q})$ *as a* $k(\mathfrak{q})$*-subalgebra.*
(iii) *If* $B = \gamma(A)B^H$ *then* $O(\mathfrak{q}) \cong k(\mathfrak{q}) \otimes_{k(\mathfrak{p})} O(\mathfrak{p})$.
(iv) *If* $\gamma a_1, \dots, \gamma a_d$ *generate* B *as a* B^H*-module for some* $a_1, \dots, a_d \in A$, *then* $\delta_{\mathfrak{p}} a_1, \dots, \delta_{\mathfrak{p}} a_d$ *span* $O(\mathfrak{p})$ *over* $k(\mathfrak{p})$.

Proof. Part (i) is seen from the commutative diagram below in which the composite of maps at the top equals $\delta_{\mathfrak{p}}$ and that at the bottom equals $\delta_{\mathfrak{q}}$:

$$\begin{array}{ccccc} A & \xrightarrow{\delta} & A \otimes H & \xrightarrow{\alpha_{\mathfrak{p}} \otimes \mathrm{id}} & k(\mathfrak{p}) \otimes H \\ \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\gamma \otimes \mathrm{id}} & & \downarrow{\scriptstyle\bar{\gamma} \otimes \mathrm{id}} \\ B & \xrightarrow{\delta} & B \otimes H & \xrightarrow{\alpha_{\mathfrak{q}} \otimes \mathrm{id}} & k(\mathfrak{q}) \otimes H. \end{array}$$

(ii) The inclusion of $O(\mathfrak{p})$ in $k(\mathfrak{p}) \otimes H$ induces an embedding of $k(\mathfrak{q})$-algebras

$$\varphi : k(\mathfrak{q}) \otimes_{k(\mathfrak{p})} O(\mathfrak{p}) \to k(\mathfrak{q}) \otimes_{k(\mathfrak{p})} (k(\mathfrak{p}) \otimes H) \cong k(\mathfrak{q}) \otimes H.$$

If $a \in A$, then $\varphi(1 \otimes \delta_{\mathfrak{p}} a) = (\bar{\gamma} \otimes \mathrm{id})(\delta_{\mathfrak{p}} a) = \delta_{\mathfrak{q}}(\gamma a)$. This shows that $\operatorname{im} \varphi \subset O(\mathfrak{q})$.

(iii) By the computation in (ii) $\delta_{\mathfrak{q}}(\gamma a) \in \operatorname{im} \varphi$ for all $a \in A$. If $b \in B^H$ then $\delta_{\mathfrak{q}} b = \alpha_{\mathfrak{q}}(b) \otimes 1 \in \operatorname{im} \varphi$ as well. Hence $\delta_{\mathfrak{q}}(B) \subset \operatorname{im} \varphi$ provided that $B = \gamma(A)B^H$. By the definition $O(\mathfrak{q}) = (k(\mathfrak{q}) \otimes 1) \cdot \delta_{\mathfrak{q}}(B) \subset \operatorname{im} \varphi$.

(iv) The hypothesis of (iii) is fulfilled, so that φ is an isomorphism. Repeating the arguments in (iii), we obtain, more precisely, that $O(\mathfrak{q})$ is spanned over $k(\mathfrak{q})$ by $\delta_{\mathfrak{q}}(\gamma a_1), \dots, \delta_{\mathfrak{q}}(\gamma a_d)$ which are the images of $1 \otimes \delta_{\mathfrak{p}} a_1, \dots, 1 \otimes \delta_{\mathfrak{p}} a_d$ under φ. Thus $O(\mathfrak{q}) = \varphi(k(\mathfrak{q}) \otimes_{k(\mathfrak{p})} V)$ where $V \subset O(\mathfrak{p})$ is the $k(\mathfrak{p})$-linear span of $\delta_{\mathfrak{p}} a_1, \dots, \delta_{\mathfrak{p}} a_d$, and so $V = O(\mathfrak{p})$. □

Remark. If $B = \gamma(A)B^H$ and $\bar{\gamma}$ is an isomorphism $k(\mathfrak{p}) \cong k(\mathfrak{q})$, then $O(\mathfrak{p}) \cong O(\mathfrak{q})$. This is the case when B is either A/I with I an H-costable ideal of A or $B = S^{-1}A$ with S a multiplicatively closed subset of A^H and γ is the canonical homomorphism in both cases. The same is true when γ is a composite of homomorphisms of these two types.

The embedding $A^H \to A$ induces a map $\pi : \operatorname{Spec} A \to \operatorname{Spec} A^H$ defined by the rule $\mathfrak{p} \mapsto \mathfrak{p} \cap A^H$ for each prime ideal $\mathfrak{p}$ of A. In the case when H is commutative, $\operatorname{Spec} A^H$ coincides with the quotient $\operatorname{Spec} A / \operatorname{Spec} H$ considered in [7,24]. The known results describing the properties of π can be extended to noncommutative Hopf algebras H.

In the rest of this section we assume that A *has invariant characteristic polynomials*. Note that the integrality of A over A^H (Proposition 2.7) implies that π is surjective and *closed*, that is, π maps closed subsets of $\operatorname{Spec} A$ onto closed subsets of $\operatorname{Spec} A^H$ [4, Chapter V, Section 2, Theorem 1, Remark 2]. A less obvious property is the *openness* of π (the open subsets of $\operatorname{Spec} A$ are mapped onto open subsets of $\operatorname{Spec} A^H$).

Theorem 3.3. *Let* $\mathfrak{p} \in \operatorname{Spec} A$. *Then*:

(i) *There are only finitely many* $\mathfrak{p}' \in \operatorname{Spec} A$ *such that* $\mathfrak{p}' \cap A^H = \mathfrak{p} \cap A^H$. *These are precisely the ideals* $\mathfrak{p}' = \delta_{\mathfrak{p}}^{-1}(\mathfrak{m})$ *for some maximal ideal* $\mathfrak{m}$ *of* $O(\mathfrak{p})$.

(ii) *The map* $\pi : \operatorname{Spec} A \to \operatorname{Spec} A^H$ *is open.*

(iii) *If* $\mathfrak{q}' \in \operatorname{Spec} A^H$ *satisfies* $\mathfrak{q}' \subset \mathfrak{p} \cap A^H$ *then* $\mathfrak{q}' = \mathfrak{p}' \cap A^H$ *for some* $\mathfrak{p}' \in \operatorname{Spec} A$ *such that* $\mathfrak{p}' \subset \mathfrak{p}$ (*Going-down property*).

Proof. In view of Lemma 1.2 the proof is reduced to the case where H is K-projective of constant rank n.

(i) Put $\mathfrak{q} = \mathfrak{p} \cap A^H$. Suppose that $\mathfrak{p}' = \delta_{\mathfrak{p}}^{-1}(\mathfrak{m})$ where $\mathfrak{m}$ is a maximal ideal of $O(\mathfrak{p})$. Then $\mathfrak{p}'$ is a prime ideal of A. Given $a \in A^H$, we have $\delta_{\mathfrak{p}}(a) = \alpha_{\mathfrak{p}}(a) \otimes 1$. Since $k(\mathfrak{p}) \otimes 1$ is a subfield in $O(\mathfrak{p})$, it has zero intersection with $\mathfrak{m}$. Hence $\delta_{\mathfrak{p}}(a) \in \mathfrak{m}$ if and only if $\alpha_{\mathfrak{p}}(a) = 0$, that is, $a \in \mathfrak{p}'$ if and only if $a \in \mathfrak{p}$. This shows that $\mathfrak{p}' \cap A^H = \mathfrak{q}$.

Suppose now that $\mathfrak{p}'$ is any prime ideal of A such that $\mathfrak{p}' \cap A^H = \mathfrak{q}$. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ be all maximal ideals of the finite-dimensional algebra $O(\mathfrak{p})$, and put $\mathfrak{p}_j = \delta_{\mathfrak{p}}^{-1}(\mathfrak{m}_j)$. Suppose that $\mathfrak{p}' \not\subset \mathfrak{p}_j$ for every j. Then $\mathfrak{p}' \not\subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_s$ by Bourbaki [4, Chapter II, Section 1, Proposition 1]. Take any $a \in \mathfrak{p}'$ outside of every $\mathfrak{p}_j$ and consider $P_{A \otimes H/A}(\delta a, t) = \sum_{i=0}^n c_i t^{n-i}$. By the assumption $c_i \in A^H$ for all i. Note that $c_n = (-1)^n N_{A \otimes H/A}(\delta a)$. As $\sum_{i=0}^n c_i a^{n-i} = 0$ (case (a) of Proposition 2.7), we have $c_n \in aA \subset \mathfrak{p}'$. Hence $c_n \in \mathfrak{q}$, and $\alpha_{\mathfrak{p}}(c_n) = 0$. On the other hand $\alpha_{\mathfrak{p}}(c_n) = (-1)^n N_{k(\mathfrak{p}) \otimes H/k(\mathfrak{p})}(\delta_{\mathfrak{p}} a)$ by (P3). By the choice of a the element $\delta_{\mathfrak{p}} a$ belongs to none of $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ and therefore is invertible in $O(\mathfrak{p})$. Then $\delta_{\mathfrak{p}} a$ is invertible also in $k(\mathfrak{p}) \otimes H$, and (P7) shows that $\alpha_{\mathfrak{p}}(c_n)$ is invertible in $k(\mathfrak{p})$, yielding a contradiction. Thus $\mathfrak{p}' \subset \mathfrak{p}_j$ for at least one j. Now $\mathfrak{p}_j \cap A^H = \mathfrak{q}$ by the previous step in the proof, and the integrality of A over A^H implies that $\mathfrak{p}' = \mathfrak{p}_j$ [4, Chapter V, Section 2, Corollary 1 to Lemma 2].

(ii) For $a \in A$ put $D_a = \{\mathfrak{p} \in \operatorname{Spec} A \mid a \notin \mathfrak{p}\}$. The subsets D_a form a base of topology on $\operatorname{Spec} A$. So it suffices to prove that $\pi(D_a)$ is an open subset of $\operatorname{Spec} A^H$ for each a. Let $P_{A \otimes H/A}(\delta a, t) = \sum_{i=0}^n c_i t^{n-i}$, so that $c_i \in A^H$ for all i. Denote by I_a the ideal of A^H generated by $c_1, \dots, c_n$. We will show that

$$\pi(D_a) = \{\mathfrak{q} \in \operatorname{Spec} A^H \mid I_a \not\subset \mathfrak{q}\}. \tag{3.2}$$

Suppose that $\mathfrak{p} \in \operatorname{Spec} A$. If $c_1, \dots, c_n \in \mathfrak{p}$ then $a^n = -\sum_{i=1}^n c_i a^{n-i} \in \mathfrak{p}$, whence $a \in \mathfrak{p}$. Therefore $a \notin \mathfrak{p}$ implies $I_a \not\subset \mathfrak{p} \cap A^H$.

Suppose that $\mathfrak{q} \in \operatorname{Spec} A^H$. Let $\mathfrak{p} \in \operatorname{Spec} A$ be any prime ideal lying above $\mathfrak{q}$. Denote by $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ all maximal ideals of $O(\mathfrak{p})$, and put $\mathfrak{p}_j = \delta_{\mathfrak{p}}^{-1}(\mathfrak{m}_j)$. By (i) $\mathfrak{p}_j \cap A^H = \mathfrak{q}$ for each j. Suppose that $a \in \mathfrak{p}_j$ for all j. Then $\delta_{\mathfrak{p}} a \in \mathfrak{m}_j$ for all j, whence $\delta_{\mathfrak{p}} a$ is a nilpotent element of $O(\mathfrak{p})$. Property (P6) yields $P_{k(\mathfrak{p}) \otimes H/k(\mathfrak{p})}(\delta_{\mathfrak{p}} a) = t^n$. On the other hand $P_{k(\mathfrak{p}) \otimes H/k(\mathfrak{p})}(\delta_{\mathfrak{p}} a, t) = \alpha_{\mathfrak{p}}^t P_{A \otimes H/A}(\delta a, t)$ by (P3), and it follows that $\alpha_{\mathfrak{p}}(c_i) = 0$, that is, $c_i \in \mathfrak{p}$ for each $i = 1, \dots, n$. Thus $I_a \not\subset \mathfrak{q}$ implies that $a \notin \mathfrak{p}_j$ for at least one j. This proves (3.2), and the openness of $\pi(D_a)$ is clear.

Part (iii) is a consequence of (ii) by Grothendieck and Dieudonné [13, Chapter I, Corollary 3.9.4] or [8] $\square$.

For $\mathfrak{p} \in \operatorname{Spec} A$ denote by $\dim O(\mathfrak{p})$ the dimension of $O(\mathfrak{p})$ as a vector space over $k(\mathfrak{p})$. We say that $\mathfrak{p}$ is *H-regular* if $\dim O(\mathfrak{p}') = \dim O(\mathfrak{p})$ for all $\mathfrak{p}'$ in a suitable neighborhood of $\mathfrak{p}$ in $\operatorname{Spec} A$.

Lemma 3.4. *Suppose that $\delta_{\mathfrak{p}} a_1, \dots, \delta_{\mathfrak{p}} a_d$ are a basis for $O(\mathfrak{p})$ over $k(\mathfrak{p})$ where $a_1, \dots, a_d \in A$. Then*:

(i) *If $\mathfrak{p}' \cap A^H = \mathfrak{p} \cap A^H$ for $\mathfrak{p}' \in \operatorname{Spec} A$ then $\delta_{\mathfrak{p}'} a_1, \dots, \delta_{\mathfrak{p}'} a_d$ are a basis for $O(\mathfrak{p}')$ over $k(\mathfrak{p}')$.*

(ii) *There exists a neighborhood U of $\mathfrak{p}$ in* Spec *A such that $\delta_{\mathfrak{p}'} a_1, \dots, \delta_{\mathfrak{p}'} a_d$ are linearly independent over $k(\mathfrak{p}')$ for each $\mathfrak{p}' \in U$.*

(iii) *If $\mathfrak{p}$ is H-regular, then there exists $s \in A^H \backslash \mathfrak{p}$ such that $\delta_{\mathfrak{p}'} a_1, \dots, \delta_{\mathfrak{p}'} a_d$ are a basis for $O(\mathfrak{p}')$ over $k(\mathfrak{p}')$ whenever $\mathfrak{p}' \in \operatorname{Spec} A$ and $s \notin \mathfrak{p}'$.*

Proof. (i) By Theorem 3.3 $\mathfrak{p}' = \delta_{\mathfrak{p}}^{-1}(\mathfrak{m})$ for some maximal ideal $\mathfrak{m}$ of $O(\mathfrak{p})$. We apply Lemma 3.2 taking $B = O(\mathfrak{p})$, $\gamma = \delta_{\mathfrak{p}}$, $\mathfrak{q} = \mathfrak{m}$, and $\mathfrak{p}'$ in place of $\mathfrak{p}$. Note that $k(\mathfrak{p}) \otimes 1 \subset B^H$. Hence the hypothesis in (iv) of Lemma 3.2 is fulfilled, and we deduce that $\delta_{\mathfrak{p}'} a_1, \dots, \delta_{\mathfrak{p}'} a_d$ span $O(\mathfrak{p}')$ over $k(\mathfrak{p}')$. It follows that $\dim O(\mathfrak{p}') \leqslant \dim O(\mathfrak{p})$. By symmetry between $\mathfrak{p}$ and $\mathfrak{p}'$ there is also the opposite inequality, which gives $\dim O(\mathfrak{p}') = d$.

(ii) There exist $k(\mathfrak{p})$-linear functions $\xi_1, \dots, \xi_d : k(\mathfrak{p}) \otimes H \to k(\mathfrak{p})$ such that $\xi_i(\delta_{\mathfrak{p}} a_j)$ is 1 when $i = j$ and 0 otherwise. Since H is a finitely projective K-module, we have

$$\operatorname{Hom}_{k(\mathfrak{p})}(k(\mathfrak{p}) \otimes H, k(\mathfrak{p})) \cong \operatorname{Hom}_K(H, k(\mathfrak{p})) \cong k(\mathfrak{p}) \otimes H^*.$$

We can find therefore $\eta_1, \dots, \eta_d \in H^*$ such that the $d \times d$ matrix with entries $(\mathrm{id} \otimes \eta_i)(\delta_{\mathfrak{p}} a_j) \in k(\mathfrak{p})$ is invertible. Denote by M and $M(\mathfrak{p}')$, where $\mathfrak{p}' \in \operatorname{Spec} A$, the $d \times d$ matrices with entries $(\mathrm{id} \otimes \eta_i)(\delta a_j) \in A$ and $(\mathrm{id} \otimes \eta_i)(\delta_{\mathfrak{p}'} a_j) \in k(\mathfrak{p}')$, respectively. Thus $M(\mathfrak{p}')$ is obtained by applying $\alpha_{\mathfrak{p}'}$ to all entries of M. Put $u = \det M \in A$. Then $\alpha_{\mathfrak{p}'}(u) = \det M(\mathfrak{p}')$, and so $M(\mathfrak{p}')$ is invertible if and only if $u \notin \mathfrak{p}'$. In particular, $u \notin \mathfrak{p}$. If $u \notin \mathfrak{p}'$ then $\delta_{\mathfrak{p}'} a_1, \dots, \delta_{\mathfrak{p}'} a_d$ are linearly independent over $k(\mathfrak{p}')$. The set $D_u = \{\mathfrak{p}' \in \operatorname{Spec} A \mid u \notin \mathfrak{p}'\}$ is the required open neighborhood of $\mathfrak{p}$ in $\operatorname{Spec} A$.

(iii) Let U be as in (ii). Taking a smaller neighborhood, if necessary, we may assume that $\dim O(\mathfrak{p}') = \dim O(\mathfrak{p})$ for all $\mathfrak{p}' \in U$. Then $\delta_{\mathfrak{p}'}a_1, \ldots, \delta_{\mathfrak{p}'}a_d$ are a basis for $O(\mathfrak{p}')$ over $k(\mathfrak{p}')$ whenever $\mathfrak{p}' \in U$. By Theorem 3.3 $\pi(U)$ is a neighborhood of $\mathfrak{q} = \mathfrak{p} \cap A^H$ in $\operatorname{Spec} A^H$. There exists $s \in A^H$ such that $\mathfrak{q} \in D_s \subset \pi(U)$, where D_s is the subset of prime ideals of A^H not containing s. If $\mathfrak{p}' \in \operatorname{Spec} A$ and $s \notin \mathfrak{p}'$ then $\mathfrak{p}' \cap A^H = \mathfrak{p}'' \cap A^H$ for some $\mathfrak{p}'' \in U$. Applying (i) with $\mathfrak{p}''$ in place of $\mathfrak{p}$, we get the desired conclusion. □

Proposition 3.5. (i) *The function* $\mathfrak{p} \mapsto \dim O(\mathfrak{p})$ *is lower semicontinuous, that is, for each integer m the subset* $\{\mathfrak{p} \in \operatorname{Spec} A \mid \dim O(\mathfrak{p}) \geqslant m\}$ *is open in* $\operatorname{Spec} A$.

(ii) *The subset of all H-regular prime ideals is dense and open in* $\operatorname{Spec} A$.

(iii) *If* $\mathfrak{p}' \cap A^H = \mathfrak{p} \cap A^H$ for $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec} A$ *then* $\dim O(\mathfrak{p}') = \dim O(\mathfrak{p})$. *For* $\mathfrak{p}'$ *to be H-regular, it is necessary and sufficient that so be* $\mathfrak{p}$.

Proof. (i) Clear from Lemma 3.4(ii).

(ii) The openness property is clear from the definition. Suppose that $U \subset \operatorname{Spec} A$ is any nonempty open subset. Put $m = \max_{\mathfrak{p} \in U} \dim O(\mathfrak{p})$. This maximum makes sense since $\dim O(\mathfrak{p}) \leqslant n$ for every $\mathfrak{p}$ where n is the number of generators for H as a K-module. The subset $V = \{\mathfrak{p} \in \operatorname{Spec} A \mid \dim O(\mathfrak{p}) \geqslant m\}$ is open by (i). Now $U \cap V$ is nonempty and consists of H-regular primes. This verifies the density property.

(iii) The equality of dimensions is proved in Lemma 3.4(i). If $\mathfrak{p}$ is H-regular and s is as in Lemma 3.4(iii), then $U = \{\mathfrak{p}'' \in \operatorname{Spec} A \mid s \notin \mathfrak{p}''\}$ is a neighborhood of $\mathfrak{p}'$ in $\operatorname{Spec} A$ such that the algebras $O(\mathfrak{p}'')$ have the same dimension for all $\mathfrak{p}'' \in U$. In this case $\mathfrak{p}'$ is H-regular. □

Lemma 3.6. *Suppose that* A^H *is local with a maximal ideal* $\mathfrak{q}$. *If there exists an H-regular* $\mathfrak{p} \in \operatorname{Spec} A$ *lying above* $\mathfrak{q}$ *then all prime ideals of A are H-regular.*

Proof. If $\mathfrak{p}'$ is any maximal ideal of A then $\mathfrak{p}' \cap A^H = \mathfrak{q}$ since A is integral over A^H. Then all maximal ideals of A are H-regular by Proposition 3.5(iii), and so are all prime ideals by (ii). □

4. Projectivity over the subring of invariants

We say that A is H-*simple* if A has no nonzero proper H-costable ideals.

Lemma 4.1. *Suppose that A is H-simple. Then* A^H *is a field and A is finite dimensional over* A^H. *If* $\mathfrak{p} \in \operatorname{Spec} A$ *and* $a_1, \ldots, a_d \in A$ *are such that* $\delta_{\mathfrak{p}}a_1, \ldots, \delta_{\mathfrak{p}}a_d$ *form a basis for* $O(\mathfrak{p})$ *over* $k(\mathfrak{p})$ *then* $a_1, \ldots, a_d$ *are a basis for A over* A^H.

Proof. The hypothesis means that A is a simple object of $\mathscr{M}_A^H$. Every A-module endomorphism of A is obtained by the rule $a \mapsto ca$ for some $c \in A$. In order that this map $A \to A$ commute with the coaction of H, it is necessary and sufficient that $c \in A^H$. In other words, A^H is identified with the endomorphism ring of A as an object of $\mathscr{M}_A^H$. By Schur's lemma A^H is a field. Given $\mathfrak{p}$, the field A^H is embedded in $k(\mathfrak{p})$. We may regard $A' = k(\mathfrak{p}) \otimes_{A^H} A$ as an object of $\mathscr{M}_A^H$ using the operations on the second tensorand. Thus $k(\mathfrak{p}) \otimes 1 \subset A'^H$. Taking any basis of $k(\mathfrak{p})$ over A^H, we present A' as a direct sum of copies of A. Hence A' is a semisimple object of $\mathscr{M}_A^H$, and every its subobject is a sum of simple subobjects isomorphic to A. Now any morphism $A \to A'$ in $\mathscr{M}_A^H$ is of the form $a \mapsto c \otimes a$ for some $c \in k(\mathfrak{p})$. So it follows that every subobject of A' is of the form $V \otimes_{A^H} A$ where $V \subset k(\mathfrak{p})$ is an A^H-subspace. Denote by $\varphi : A' \to k(\mathfrak{p}) \otimes H$ the $k(\mathfrak{p})$-linear map extending $\delta_\mathfrak{p} : A \to k(\mathfrak{p}) \otimes H$. Then φ is a homomorphism of H-comodule algebras, and so $I = \ker \varphi$ is an H-costable ideal of A'. Hence I is a subobject of A' in $\mathscr{M}_A^H$. We deduce that $I = V \otimes_{A^H} A$ for some V as above. On the other hand, φ is injective on $k(\mathfrak{p}) \otimes 1$. Since $V \otimes 1 \subset I$, we get $V = 0$. Thus φ is injective. The image of φ coincides with $O(\mathfrak{p})$ by the definition. If $\delta_\mathfrak{p} a_1, \dots, \delta_\mathfrak{p} a_d$ form a basis for $O(\mathfrak{p})$ over $k(\mathfrak{p})$ then $1 \otimes a_1, \dots, 1 \otimes a_d$ form a basis for A' over $k(\mathfrak{p})$, and the final assertion is clear. $\square$

Lemma 4.2. *Suppose that A has a maximal ideal $\mathfrak{p}$ which contains no nonzero H-costable ideals of A. Then A is H-simple.*

Proof. The H-radical of A is contained in every prime ideal of A. The hypothesis of the lemma implies therefore that A is H-reduced. By Theorem 2.5 A is integral over A^H. Next, the ideal of A generated by $\mathfrak{p} \cap A^H$ is H-costable and is contained in $\mathfrak{p}$. Hence $\mathfrak{p} \cap A^H = 0$. The maximality of $\mathfrak{p}$ ensures that (0) is a maximal ideal of A^H [4, Chapter V, Section 2, Proposition 1]. In other words A^H is a field. Suppose that I is any proper H-costable ideals of A. Then $I \subset \mathfrak{p}'$ for some maximal ideal $\mathfrak{p}'$ of A. By Lemma 3.1 $\delta_{\mathfrak{p}'}(I) = 0$. As $\mathfrak{p}' \cap A^H = 0$, Theorem 3.3 shows that $\mathfrak{p} = \delta_{\mathfrak{p}'}^{-1}(\mathfrak{m})$ for some maximal ideal $\mathfrak{m}$ of $O(\mathfrak{p}')$. But then $I \subset \mathfrak{p}$, and so $I = 0$ by the hypothesis. $\square$

Denote by $\mathscr{M}'$ the full subcategory of $\mathscr{M}_A^H$ consisting of right (H, A)-Hopf modules M such that $M = M^H A$. The next result generalizes [28, Theorem 2.1, Proposition 3.2] where K was supposed to be an algebraically closed field, A a finitely generated integral domain and H a commutative Hopf algebra.

Theorem 4.3. *Suppose that A is H-reduced and the function $\mathfrak{p} \mapsto \dim O(\mathfrak{p})$ is locally constant on the whole* Spec A. *Then*:

(i) *A is a finitely generated projective A^H-module whose rank at $\mathfrak{q} \in \operatorname{Spec} A^H$ is equal to* $\dim O(\mathfrak{p})$ *where $\mathfrak{p}$ is any prime ideal of A lying above $\mathfrak{q}$.*

(ii) *The functor $M \mapsto M^H$ is an equivalence between $\mathscr{M}'$ and the category of A^H-modules. The inverse functor is $N \mapsto N \otimes_{A^H} A$.*

(iii) *The assignment $I \mapsto I \cap A^H$ establishes a bijection between the H-costable ideals of A and the ideals of A^H. The inverse correspondence is $J \mapsto JA$.*

Proof. For every $s \in A^H$ the localization A_s is an H-reduced H-comodule algebra. Given $M \in \mathscr{M}_A^H$, one has $M_s \in \mathscr{M}_{A_s}^H$ by Lemma 1.1. If, moreover, $M = M^H A$ then $M_s = M_s^H A$. To prove (i) it suffices, by Bourbaki [4, Chapter II, Section 5, Theorem 1], to show that for every $\mathfrak{q} \in \operatorname{Spec} A^H$ there exists $s \in A^H$ such that $s \notin \mathfrak{q}$ and A_s is a free A_s^H-module of rank $d = \dim O(\mathfrak{p})$ (by Proposition 3.5 d does not depend on a choice of $\mathfrak{p}$ above $\mathfrak{q}$). In (ii) one first notes that the two functors are well defined; the H-comodule structure on $N \otimes_{A^H} A$ is given by means of the map

$$\mathrm{id} \otimes \delta : N \otimes_{A^H} A \to N \otimes_{A^H} (A \otimes H) \cong (N \otimes_{A^H} A) \otimes H.$$

For every $M \in \mathscr{M}'$ and every A^H-module N define

$$\Psi_M : M^H \otimes_{A^H} A \to M, \quad \Phi_N : N \to (N \otimes_{A^H} A)^H.$$

by $v \otimes a \mapsto va$ and $v \mapsto v \otimes 1$, respectively. Then Ψ_M is a morphism in $\mathscr{M}'$ and Φ_N is a homomorphism of A^H-modules. The map Ψ_M is bijective if and only if for every $\mathfrak{q} \in \operatorname{Spec} A^H$ there exists $s \in A^H$ such that $s \notin \mathfrak{q}$ and $\Psi_M \otimes_A A_s$ is bijective (cf. [4, Chapter II, Section 3, Theorem 1]). Note that $\Psi_M \otimes_A A_s$ can be identified with the map $M_s^H \otimes_{A_s^H} A_s \to M_s$ such that $v \otimes a \mapsto va$. The bijectivity of Φ_N can be verified similarly. Thus, in proving (i) and (ii), we may pass to suitable localizations A_s.

By the hypothesis all prime ideals of A are H-regular. Taking s as in Lemma 3.4(iii) with respect to any chosen prime ideal of A and replacing A with A_s, we reduce the proof to the case in which there exist $a_1, \ldots, a_d \in A$ such that for every $\mathfrak{p} \in \operatorname{Spec} A$ the elements $\delta_{\mathfrak{p}} a_1, \ldots, \delta_{\mathfrak{p}} a_d$ form a basis for $O(\mathfrak{p})$ over $k(\mathfrak{p})$. We fix $a_1, \ldots, a_d$.

Let us regard $A \otimes H$ as an A-module via left multiplications on the first tensorand. This module is finitely projective since so is the K-module H. Consider its submodule $E \subset A \otimes H$ generated by $\delta a_1, \ldots, \delta a_d$. If $\mathfrak{p} \in \operatorname{Spec} A$ then the $A_{\mathfrak{p}}$-module $A_{\mathfrak{p}} \otimes H$ obtained by localizing $A \otimes H$ at $\mathfrak{p}$ is free of finite rank. Furthermore, $E_{\mathfrak{p}}$ may be identified with an $A_{\mathfrak{p}}$-submodule of $A_{\mathfrak{p}} \otimes H$ generated by d elements whose images in $k(\mathfrak{p}) \otimes H$ are linearly independent over $k(\mathfrak{p})$. Then $E_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-module direct summand of $A_{\mathfrak{p}} \otimes H$ [4, Chapter II, Section 3, Corollary 1 to Proposition 5]. In particular, $E_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of finite rank. If $\varphi : A^d \to E$ is the A-module homomorphism sending the standard generators of the rank d free A-module A^d to $\delta a_1, \ldots, \delta a_d$ then the localizations of φ at prime ideals of A are all isomorphisms. Hence φ is itself an isomorphism, i.e., E is a free A-module with $\delta a_1, \ldots, \delta a_d$ as its basis. By Bourbaki [4, Chapter II, Section 3, Corollary 1 to Proposition 12] E is an A-module direct summand of $A \otimes H$.

Claim 1. *Let $I(\mathfrak{p})$ be the largest H-costable ideal of A contained in a prime ideal $\mathfrak{p}$. Then $\delta(A) \subset E + I(\mathfrak{p}) \otimes H$.*

Put $I = I(\mathfrak{p})$ and $\mathfrak{q} = \mathfrak{p} \cap A^H$. The prime ideal $\mathfrak{p} A_{\mathfrak{q}}$ of $A_{\mathfrak{q}}$ lies above the maximal ideal $\mathfrak{q} A_{\mathfrak{q}}^H$ of $A_{\mathfrak{q}}^H$. By Theorem 2.5 $A_{\mathfrak{q}}$ is integral over $A_{\mathfrak{q}}^H$, whence $\mathfrak{p} A_{\mathfrak{q}}$ is a maximal ideal of $A_\mathfrak{q}$. Next, $IA_\mathfrak{q}$ is the largest H-costable ideal of $A_\mathfrak{q}$ contained in $\mathfrak{p}A_\mathfrak{q}$. Lemma 4.2 shows that the H-comodule algebra $A' = A_\mathfrak{q}/IA_\mathfrak{q}$ is H-simple. If $\mathfrak{p}' = \mathfrak{p}A_\mathfrak{q}/IA_\mathfrak{q}$, then there is an isomorphism $O(\mathfrak{p}) \to O(\mathfrak{p}')$ (see Lemma 3.2) such that $\delta_\mathfrak{p} a_i \mapsto \delta_{\mathfrak{p}'} a'_i$ where a'_i denotes the image of a_i in A' for each $i = 1, \dots, d$. Hence $\delta_{\mathfrak{p}'} a'_1, \dots, \delta_{\mathfrak{p}'} a'_d$ form a basis for $O(\mathfrak{p}')$ over $k(\mathfrak{p}')$. Applying Lemma 4.1, we deduce that A' is spanned over A'^H by $a'_1, \dots, a'_d$. As $\delta(A'^H) \subset A' \otimes 1$, it follows that $\delta(A')$ is contained in the A'-submodule $E' \subset A' \otimes H$ generated by $\delta a'_1, \dots, \delta a'_d$. Clearly E' coincides with the image of the localization $E_\mathfrak{q}$ under canonical map $A_\mathfrak{q} \otimes H \to A' \otimes H$. The kernel of the latter map is $IA_\mathfrak{q} \otimes H$. Hence

$$\delta(A_\mathfrak{q}) \subset E_\mathfrak{q} + IA_\mathfrak{q} \otimes H. \tag{4.1}$$

Put $J = \{b \in A \mid ub \in I \text{ for some } u \in A^H \backslash \mathfrak{q}\}$. For every projective A-module P we have

$$JP = \{x \in P \mid ux \in IP \text{ for some } u \in A^H \backslash \mathfrak{q}\} \tag{4.2}$$

(this is clear for free A-modules, hence also for their direct summands). If $b \in J$ and $ub \in I$ for $u \in A^H \backslash \mathfrak{q}$ then $(u \otimes 1)\delta(b) = \delta(ub) \in I \otimes H$. Equality (4.2) applied to $P = A \otimes H$ yields $\delta(b) \in J \otimes H$. Thus J is an H-costable ideal of A. On the other hand, $J \subset \mathfrak{p}$ since $I \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime. It follows that $J \subset I$ by the maximality of I. In fact $J = I$ since the opposite inclusion is obvious. Let $a \in A$. By (4.1) there exists $u \in A^H \backslash \mathfrak{q}$ such that $(u \otimes 1)\delta(a) \in E + I \otimes H$. Taking $P = (A \otimes H)/E$, we deduce from (4.2) that $\delta(a) \in E + J \otimes H = E + I \otimes H$. Claim 1 is proved.

Claim 2. *Put $B = (A \otimes 1) \cdot \delta(A) \subset A \otimes H$. Then B is an A-module direct summand of $A \otimes H$ and is a free A-module with $\delta a_1, \dots, \delta a_d$ as its basis.*

Put $J = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} I(\mathfrak{p})$. Then

$$JP = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} I(\mathfrak{p})P \tag{4.3}$$

for every projective A-module P (the verification reduces again to free A-modules). Taking $P = A \otimes H$, we see that $\delta(J) \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} I(\mathfrak{p}) \otimes H = J \otimes H$. Thus J is an H-costable ideal of A. Since $J \subset \mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{Spec} A$, all elements of J are nilpotent. Hence $J = 0$ by the assumption on A. Using Claim 1 and (4.3) with $P = (A \otimes H)/E$, we get

$$\delta(A) \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} (E + I(\mathfrak{p}) \otimes H) = E + J \otimes H = E.$$

Hence $B \subset E$ as well. Then $B = E$ since the opposite inclusion is obvious. This completes the proof of Claim 2.

For each A-module M consider $M \otimes H$ as an $A \otimes H$-module by means of the operation $(v \otimes g)(a \otimes h) = va \otimes gh$ where $v \in M$, $a \in A$ and $g, h \in H$. Put $E_M = (M \otimes 1) \cdot \delta(A) \subset M \otimes H$, which is a B-submodule. Clearly E_M coincides with the image of the map

$$M \otimes_A B \to M \otimes_A (A \otimes H) \cong M \otimes H$$

induced by the inclusion of B into $A \otimes H$. Since B is an A-module direct summand of $A \otimes H$, the map above is injective, and so $E_M \cong M \otimes_A B$.

Claim 3. *Each element of E_M can be written as $\sum_{i=1}^d (v_i \otimes 1) \cdot \delta(a_i)$ with uniquely determined $v_1, \ldots, v_d \in M$.*

This is immediate from the freeness of B over A.

Claim 4. *If $M \in \mathscr{M}'$ then each element of M can be written as $\sum_{i=1}^d v_i a_i$ with uniquely determined $v_1, \ldots, v_d \in M^H$.*

If $v_1, \ldots, v_d \in M^H$ and $\sum v_i a_i = 0$ then $\sum (v_i \otimes 1)\delta(a_i) = \delta(\sum v_i a_i) = 0$ in E_M, whence $v_1 = \cdots = v_d = 0$ by Claim 3. This verifies the uniqueness. Next, we have $\delta(M) = \delta(M^H A) = (M^H \otimes 1)\delta(A) \subset E_M$. Given $u \in M$, there exist therefore $v_1, \ldots, v_d \in M$ such that

$$\delta u = \sum (v_i \otimes 1) \cdot \delta(a_i). \tag{4.4}$$

Applying $\mathrm{id} \otimes \varepsilon$ to both sides of this equality, we get $u = \sum v_i a_i$ since $(\mathrm{id}_X \otimes \varepsilon) \circ \delta = \mathrm{id}_X$ for both $X = M$ and $X = A$. Applying $\delta \otimes \mathrm{id}_H$ and $\mathrm{id}_M \otimes \Delta$ to both sides of (4.4), and taking into account the identity $(\delta \otimes \mathrm{id}) \circ \delta = (\mathrm{id} \otimes \Delta) \circ \delta$, we get

$$\sum (\delta v_i \otimes 1) \cdot (\delta \otimes \mathrm{id})\delta a_i = \sum (v_i \otimes 1 \otimes 1) \cdot (\delta \otimes \mathrm{id})\delta a_i \tag{4.5}$$

in $M \otimes H \otimes H$. Here we consider $M \otimes H \otimes H$ as a right $A \otimes H \otimes H$-module in a natural way. Let W denote the A-module $M \otimes H$ on which A operates via the ring homomorphism $\delta : A \to A \otimes H$. Then $A \otimes H$ operates on $W \otimes H \cong M \otimes H \otimes H$ via the ring homomorphism $\delta \otimes \mathrm{id}_H$, and (4.5) can be rewritten as an equality $\sum (w_i \otimes 1) \cdot \delta(a_i) = 0$ in E_W where $w_i = \delta v_i - v_i \otimes 1 \in W$. Claim 3 yields $\delta v_i = v_i \otimes 1$, that is, $v_i \in M^H$ for all i. Thus u has the required form, and Claim 4 is proved.

Note that A can be regarded as an object of $\mathscr{M}_A^H$. Moreover, $A \in \mathscr{M}'$ since $1 \in A^H$. We see, in particular, that each element $a \in A$ can be uniquely written as $\sum c_i a_i$ with $c_1, \ldots, c_d \in A^H$. In other words, A is a free A^H-module with $a_1, \ldots, a_d$ as its basis.

Now $M^H \otimes_{A^H} A \cong M^H \oplus \ldots \oplus M^H$ (d copies), and the restriction of Ψ_M to the ith summand is given by the map $v \mapsto v a_i$. Claim 4 shows that Ψ_M is bijective.

Suppose that N is any A^H-module and $M = N \otimes_{A^H} A$. The composite

$$N \otimes_{A^H} A \xrightarrow{\Phi_N \otimes \mathrm{id}} M^H \otimes_{A^H} A \xrightarrow{\Psi_M} M$$

is then the identity transformation of M. Since Ψ_M is bijective, so too is $\Phi_N \otimes \mathrm{id}$. Since A is a free A^H-module, Φ_N is bijective as well. The proof of (i) and (ii) is now complete.

If I is an H-costable ideal of A, then $A/I \in \mathscr{M}'$. As the canonical map $A \to A/I$ is an epimorphism in $\mathscr{M}'$, the corresponding map $A^H \to (A/I)^H$ is an epimorphism of A^H-modules by (ii). Thus $(A/I)^H \cong A^H/I^H$. In the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & I^H \otimes_{A^H} A \arrow[r] & A^H \otimes_{A^H} A \arrow[r] \arrow[d, "\Psi_A"'] & A^H/I^H \otimes_{A^H} A \arrow[r] \arrow[d, "\Psi_{A/I}"'] & 0 \\ 0 \arrow[r] & I \arrow[r] & A \arrow[r] & A/I \arrow[r] & 0 \end{tikzcd}$$

the rows are exact by freeness of A over A^H and the vertical arrows are bijective by (ii). Hence Ψ_A induces a bijection $I^H \otimes_{A^H} A \cong I$, which shows that $I = I^H A$. Thus I is an $\mathscr{M}'$-subobject of A. By (ii) the $\mathscr{M}'$-subobjects of A are in a bijective correspondence with the ideals of A^H, and (iii) follows. □

Corollary 4.4. *If A is H-reduced and $\mathfrak{p} \in \operatorname{Spec} A$ is H-regular then there is an isomorphism of $k(\mathfrak{p})$-algebras $O(\mathfrak{p}) \cong k(\mathfrak{p}) \otimes_{k(\mathfrak{q})} A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}$ where $\mathfrak{q} = \mathfrak{p} \cap A^H$.*

Proof. In view of Lemma 3.2 we may replace A with $A_\mathfrak{q}$ and $\mathfrak{p}$ with $\mathfrak{p}A_\mathfrak{q}$. So we may assume that A^H is local and $\mathfrak{q}$ is its maximal ideal. Then all prime ideals of A are H-regular by Lemma 3.6, so that the hypotheses of Theorem 4.3 are fulfilled. It follows that A is a free A^H-module of rank $d = \dim O(\mathfrak{p})$. Then $\dim_{k(\mathfrak{q})} A/\mathfrak{q}A = d$. By Lemma 3.1 $\mathfrak{q} \subset \ker \delta_\mathfrak{p}$. Therefore $\delta_\mathfrak{p}$ extends to a homomorphism of $k(\mathfrak{p})$-algebras $\varphi : k(\mathfrak{p}) \otimes_{k(\mathfrak{q})} A/\mathfrak{q}A \to O(\mathfrak{p})$ which is clearly surjective. Comparing the dimensions, we deduce that φ is bijective. □

Consider the map $\gamma : A \otimes A \to A \otimes H$ such that $a \otimes b \mapsto (a \otimes 1) \cdot \delta(b)$. One says that A is an *H-Galois extension of A^H* if γ is surjective [6,18]. In this case γ induces a bijection $A \otimes_{A^H} A \cong A \otimes H$.

Proposition 4.5. *A is an H-Galois extension of A^H if and only if $O(\mathfrak{p}) = k(\mathfrak{p}) \otimes H$ for all $\mathfrak{p} \in \operatorname{Spec} A$, if and only if $O(\mathfrak{p}) = k(\mathfrak{p}) \otimes H$ for all maximal ideals $\mathfrak{p}$ of A.*

Proof. The map γ is A-linear with respect to the actions of A by multiplications on the first tensorands. If γ is surjective then so too is $k(\mathfrak{p}) \otimes_A \gamma$ for every $\mathfrak{p} \in \operatorname{Spec} A$. The latter can be identified with the map $\gamma_\mathfrak{p} : k(\mathfrak{p}) \otimes A \to k(\mathfrak{p}) \otimes H$ such that $c \otimes b \mapsto (c \otimes 1)\delta_\mathfrak{p}(b)$. The image of $\gamma_\mathfrak{p}$ coincides with $O(\mathfrak{p})$, and therefore $\gamma_\mathfrak{p}$ is surjective if and only if $O(\mathfrak{p}) = k(\mathfrak{p}) \otimes H$. Note that the A-module $A \otimes H$ is finitely generated since so is the K-module H. By Bourbaki [4, Chapter II, Section 3, Proposition 11] γ is surjective whenever the maps $\gamma_\mathfrak{p}$ are surjective for all maximal ideals of A. □

Remark. If A is H-Galois then $\dim O(\mathfrak{p}) = \mathrm{rk}_{\mathfrak{p}\cap K} H$. The function $\mathfrak{p} \mapsto \dim O(\mathfrak{p})$ is therefore locally constant in this case. In fact, the conclusions of Theorem 4.3 are valid for an H-Galois A under much weaker assumptions. One need not assume A to be either H-reduced or even commutative. If A is H-Galois, then A is finitely projective as a left and as a right A^H-module [18, (1.7), (1.8)]. Moreover, the functor $M \mapsto M^H$ establishes an equivalence between $\mathscr{M}_A^H$ and the category of A^H-modules provided that A is a faithfully flat left A^H-module (this is automatic when A is commutative) [27, Theorem 3.7]; similar results can be found in [11, (2.11)], [30, p. 661]. If A and H are commutative, then the condition that A is H-Galois means precisely that the finite group scheme $\operatorname{Spec} H$ operates freely on $\operatorname{Spec} A$. The corresponding results on the quotient of this action are contained in [7, Chapter III, Section 12], [24, Chapter III, Section 2]. Thus Theorem 4.3 generalizes these classical results.

Lemma 4.6. *Suppose that A is H-reduced and Noetherian. Let $\mathfrak{p} \in \operatorname{Spec} A$ be H-regular, and let $a_1, \dots, a_d \in A$ be elements such that $\delta_{\mathfrak{p}} a_1, \dots, \delta_{\mathfrak{p}} a_d$ form a basis for $O(\mathfrak{p})$ over $k(\mathfrak{p})$. Then there exist $s \in A^H \backslash \mathfrak{p}$ and an integer $n > 0$ such that $s^n A \subset A^H a_1 + \cdots + A^H a_d$.*

Proof. Let s be as in Lemma 3.4(iii). Put

$$B = (A \otimes 1) \cdot \delta(A) \quad \text{and} \quad E = \sum_{i=1}^{d} (A \otimes 1) \cdot \delta(a_i)$$

so that $E \subset B \subset A \otimes H$. Both B and E are A-submodules of $A \otimes H$ with respect to the action of A by left multiplications on the first tensorand. Localizing at s, we obtain a chain of A_s-modules $E_s \subset B_s \subset A_s \otimes H$. Clearly $B_s = (A_s \otimes 1) \cdot \delta(A_s)$ and $E_s = \sum_{i=1}^{d} (A_s \otimes 1) \cdot \delta(a_i')$ where a_i' denotes the image of a_i in A_s. The H-comodule algebra A_s fulfills the hypotheses under which Claim 2 in the proof of Theorem 4.3 was verified. This claim shows that B_s is an A_s-module direct summand of $A_s \otimes H$ and B_s is a free A_s-module with $\delta(a_1'), \dots, \delta(a_d')$ as its basis. In particular, $B_s = E_s$. Now B is a finitely generated A-module since so is $A \otimes H$ and A is Noetherian. Hence there exists an integer $m > 0$ such that $(s^m \otimes 1) \cdot B \subset E$.

Let F be a free A-module with a basis $e_1, \dots, e_d$. Consider the A-module homomorphism $\varphi : F \to A \otimes H$ such that $e_i \mapsto \delta(a_i)$ for each $i = 1, \dots, d$, and put $R = \ker \varphi$. The localization of φ at s is an isomorphism of F_s onto B_s, whence $R_s = 0$. The A-module R is finitely generated as A is Noetherian. It follows that there exists an integer $l > 0$ such that $s^l R = 0$. Taking $n = m + l$, we will show that the conclusion of the lemma is fulfilled.

Put $T = A \otimes H$ considered as a ring extension of A by means of the ring homomorphism $\delta : A \to A \otimes H$. We claim that T is a projective right A-module with respect to δ. The K-linear transformation v of $A \otimes H$ such that $a \otimes h \mapsto (1 \otimes h) \cdot \delta a$ for $a \in A$ and $h \in H$ is invertible (the assignment $a \otimes h \mapsto (1 \otimes h) \cdot (\mathrm{id} \otimes \sigma^{-1})(\delta a)$

defines the inverse transformation). As $v(ab\otimes h)=v(a\otimes h)\cdot\delta b$ for all $a,b\in A$ and $h\in H$, one sees that v is an isomorphism between the two A-module structures on $A\otimes H$ obtained via ring homomorphisms $b\mapsto b\otimes 1$ and δ, respectively. As H is K-projective, $A\otimes H$ is projective with respect to the first of these two module structures, hence also with respect to the second one.

By projectivity of T over A we obtain an exact sequence of T-modules

$$0\to T\otimes_A R\to T\otimes_A F\xrightarrow{\psi} T\otimes_A(A\otimes H)\cong T\otimes H\cong A\otimes H\otimes H,$$

where $\psi=\mathrm{id}\otimes\varphi$ and the isomorphisms shown are such that $y\otimes z$ in $T\otimes_A(A\otimes H)$ goes to $(y\otimes 1)\cdot(\delta\otimes\mathrm{id})(z)$ in $A\otimes H\otimes H$ where $y,z\in A\otimes H$. As $\delta s=s\otimes 1$ is in the center of T, we get

$$(s^l\otimes 1)T\otimes_A R=T\delta(s^l)\otimes_A R=T\otimes_A s^l R=0.$$

Note that $\psi(1\otimes e_i)=(\delta\otimes\mathrm{id})(\delta a_i)$ in $A\otimes H\otimes H$ for each $i=1,\dots,d$. Given $x_1,\dots,x_d\in T$, we deduce that

$$\sum (x_i\otimes 1)\cdot(\delta\otimes\mathrm{id})(\delta a_i)=0\Rightarrow\sum x_i\otimes e_i\in\ker\psi\Rightarrow(s^l\otimes 1)x_i=0. \tag{4.6}$$

Let now $a\in A$ be any element, and put $b=s^m a$. Then $\delta b=(s^m\otimes 1)\cdot\delta a\in E$. We can write therefore $\delta b=\sum(c_i\otimes 1)\cdot\delta a_i$ for some $c_1,\dots,c_d\in A$. Applying $\mathrm{id}\otimes\varepsilon$ to both sides of this equality, we get $b=\sum c_i a_i$. Applying $\delta\otimes\mathrm{id}_H$ and $\mathrm{id}_A\otimes\Delta$, we get

$$\sum (\delta c_i\otimes 1)\cdot(\delta\otimes\mathrm{id})\delta a_i=\sum (c_i\otimes 1\otimes 1)\cdot(\delta\otimes\mathrm{id})\delta a_i$$

in $A\otimes H\otimes H$ (cf. the proof of Claim 4 in Theorem 4.3). Now (4.6) shows that $(s^l\otimes 1)\cdot(\delta c_i-c_i\otimes 1)=0$ for each $i=1,\dots,d$. The last equalities can be rewritten as $\delta(s^l c_i)=s^l c_i\otimes 1$, which shows that $s^l c_i\in A^H$ for each i. We deduce that $s^n a=s^l b=\sum s^l c_i a_i$ is of required form. $\square$

5. Semisimple stabilizer subalgebras and total integrals

For each $\mathfrak{p}\in\operatorname{Spec} A$ consider the left coideal subalgebra $\mathrm{St}(\mathfrak{p})\subset k(\mathfrak{p})\otimes H^*$ corresponding to the right coideal subalgebra $O(\mathfrak{p})\subset k(\mathfrak{p})\otimes H$ (see Proposition 1.6). We call $\mathrm{St}(\mathfrak{p})$ the *stabilizer subalgebra* associated with $\mathfrak{p}$. This name is justified by the next lemma. We may regard $k(\mathfrak{p})\otimes A$ as an H-comodule algebra with respect to the map $\mathrm{id}\otimes\delta$ or as a comodule algebra for the Hopf algebra $k(\mathfrak{p})\otimes H$ over $k(\mathfrak{p})$. Then $k(\mathfrak{p})\otimes A$ is also a module over $k(\mathfrak{p})\otimes H^*$.

Lemma 5.1. *Put $A'=k(\mathfrak{p})\otimes A$, and let $\alpha'_\mathfrak{p}:A'\to k(\mathfrak{p})$ be the homomorphism of $k(\mathfrak{p})$-algebras which extends the canonical ring homomorphism $\alpha_\mathfrak{p}:A\to k(\mathfrak{p})$. Then $\mathfrak{p}'=$*

$\ker \alpha'_{\mathfrak{p}}$ *is a maximal ideal of* A' *such that* $k(\mathfrak{p}') \cong k(\mathfrak{p})$ *and* $\mathrm{St}(\mathfrak{p}') \cong \mathrm{St}(\mathfrak{p})$. *Furthermore,* $\mathrm{St}(\mathfrak{p})$ *is the largest left coideal of* $k(\mathfrak{p}) \otimes H^*$ *which leaves* $\mathfrak{p}'$ *stable.*

Proof. Clearly $A'/\mathfrak{p}' \cong k(\mathfrak{p})$ so that $\mathfrak{p}'$ is a maximal ideal of A' with residue field $k(\mathfrak{p})$. The map $\gamma : A \to A'$ defined by the rule $a \mapsto 1 \otimes a$ for $a \in A$ is a homomorphism of H-comodule algebras. Since $\alpha'_{\mathfrak{p}} \circ \gamma = \alpha_{\mathfrak{p}}$, we have $\gamma^{-1}(\mathfrak{p}') = \ker \alpha_{\mathfrak{p}} = \mathfrak{p}$ and γ induces an isomorphism $k(\mathfrak{p}) \cong k(\mathfrak{p}')$. Since $k(\mathfrak{p}) \otimes 1 \subset A'^H$, Lemma 3.2 yields an isomorphism $O(\mathfrak{p}) \cong O(\mathfrak{p}')$. Then $\mathrm{St}(\mathfrak{p}) \cong \mathrm{St}(\mathfrak{p}')$ as well. To complete the proof of the lemma we may pass to base ring $k(\mathfrak{p})$ replacing $\mathfrak{p}$, A, H with $\mathfrak{p}'$, A', $k(\mathfrak{p}) \otimes H$, respectively. Thus it suffices to consider the case where K is a field and $\mathfrak{p}$ is a maximal ideal of A such that $k(\mathfrak{p}) \cong K$.

In this case $O(\mathfrak{p}) = \delta_{\mathfrak{p}}(A)$. Since $\varepsilon \circ \delta_{\mathfrak{p}} = \alpha_{\mathfrak{p}}$ as shown in diagram (3.1), we see that $\delta_{\mathfrak{p}}(a) \in O(\mathfrak{p})^+$ for $a \in A$ if and only if $a \in \ker \alpha_{\mathfrak{p}} = \mathfrak{p}$. Hence $O(\mathfrak{p})^+ = \delta_{\mathfrak{p}}(\mathfrak{p})$. For $\mathfrak{p}$ to be stable under the action of $\xi \in H^*$ it is necessary and sufficient that $(\alpha_{\mathfrak{p}} \circ L_\xi)(\mathfrak{p}) = 0$ where L_ξ is the transformation of A shown in (1.2). Since

$$\alpha_{\mathfrak{p}} \circ L_\xi = (\alpha_{\mathfrak{p}} \otimes \xi) \circ \delta = \xi \circ \delta_{\mathfrak{p}},$$

this condition can be rewritten as $\xi(O(\mathfrak{p})^+) = 0$. Suppose that $C \subset H^*$ is a left coideal consisting of linear functions which vanish on $O(\mathfrak{p})^+$. If $\xi \in C$ and $h \in H$ then $\xi \leftharpoonup h \in C$ where $\xi \leftharpoonup h \in H^*$ is defined by the rule $(\xi \leftharpoonup h)(g) = \xi(hg)$ for $g \in H$. Hence all $\xi \in C$ vanish on $H \cdot O(\mathfrak{p})^+$ and so belong to $\mathrm{St}(\mathfrak{p})$. $\square$

Remark. Note that in the situation of Proposition 1.6 $\dim C = \dim H/HB^+ = \mathrm{rk}_B H = \dim H/\dim B$. Applying this fact to the orbital subalgebras, we deduce that

$$\dim O(\mathfrak{p}) \cdot \dim \mathrm{St}(\mathfrak{p}) = \dim k(\mathfrak{p}) \otimes H = \mathrm{rk}_{\mathfrak{p} \cap K} H.$$

One may regard H as a right H-comodule via Δ. Any H-comodule homomorphism $\varphi : H \to A$ is called an *integral*. If, in addition, $\varphi(1) = 1$ then φ is a *total integral*. As was observed by Doi [9] the comodule algebras admitting a total integral enjoy remarkable properties. An H-comodule W is called *relatively injective* if, whenever U is an H-costable K-module direct summand of an H-comodule V, every H-comodule map $U \to W$ can be extended to an H-comodule map $V \to W$.

Proposition 5.2. *The following conditions are equivalent*:

(i) *All objects* $M \in \mathcal{M}_A^H$ *are relatively injective* H*-comodules.*
(ii) A *is a relatively injective* H*-comodule.*
(iii) *There exists a total integral* $\varphi : H \to A$.
(iv) *There exist natural* K*-linear retractions* $\mathrm{tr}_M : M \to M^H$, *defined for each* $M \in \mathcal{M}_A^H$.
(v) *The functor* $M \mapsto M^H$ *is exact on* $\mathcal{M}_A^H$.
(vi) A *is a projective object of* $\mathcal{M}_A^H$.

Proof. Equivalences (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) are proved in [9, (1.6)].

(iii) $\Rightarrow$ (iv): Denote by tr_M the composite

$$M \xrightarrow{\delta} M \otimes H \xrightarrow{\mathrm{id} \otimes \sigma} M \otimes H \xrightarrow{\mathrm{id} \otimes \varphi} M \otimes A \to M,$$

where the last map is afforded by the A-module structure on M. As was shown in [10, Section 1] $\mathrm{tr}_M(M) \subset M^H$ and all required properties are fulfilled.

(iv) $\Rightarrow$ (v): The functor $M \mapsto M^H$ is clearly left exact. Suppose that $\xi : M \to N$ is an epimorphism in $\mathscr{M}_A^H$. Given $u \in N^H$, take $v \in M$ such that $\xi(v) = u$. Then $\mathrm{tr}_M(v) \in M^H$ and $\xi(\mathrm{tr}_M(v)) = \mathrm{tr}_N(\xi(v)) = u$. Thus ξ induces a surjection $M^H \to N^H$.

(v) $\Leftrightarrow$ (vi): This is clear since every morphism $A \to M$ in $\mathscr{M}_A^H$ is given by the rule $a \mapsto va$ where $v \in M^H$.

(v) $\Rightarrow$ (iii): If V, W are two K-modules and V is finitely projective, then there is a canonical bijection $\alpha_{VW} : V^* \otimes W \to \mathrm{Hom}_K(V, W)$ where $V^* = \mathrm{Hom}_K(V, K)$. Suppose that V, W are, moreover, H-comodules. Define an H-comodule structure on V^* such that $\delta\eta \in V^* \otimes H$, where $\eta \in V^*$, corresponds under bijection α_{VH} to the composite K-linear map

$$V \xrightarrow{\delta} V \otimes H \xrightarrow{\eta \otimes \sigma^{-1}} K \otimes H \cong H$$

(note that the antipode σ of H is bijective by Pareigis [26, Proposition 4]). If $V^* \otimes W$ is equipped with the tensor product of two comodule structures, then α_{VW} maps $(V^* \otimes W)^H$ bijectively onto the set $\mathrm{Com}(V, W)$ of all H-comodule homomorphisms $V \to W$. As a special case we have $V^* \otimes A \in \mathscr{M}_A^H$ where A operates by multiplications on the second tensorand. Now K is a K-module direct summand of H as $\varepsilon : H \to K$ is a retraction. Moreover, K is an H-subcomodule of H. Then the restriction map $H^* \to K^*$ is an epimorphism of H-comodules which gives rise to an epimorphism $H^* \otimes A \to K^* \otimes A$ in $\mathscr{M}_A^H$. Taking the invariants, we deduce that the restriction map $\mathrm{Com}(H, A) \to \mathrm{Com}(K, A)$ is surjective. In particular, the H-comodule map $K \to A$ such that $1 \mapsto 1$ extends to an integral $\varphi : H \to A$. $\square$

Remark. The commutativity of A is not needed in this result. The assumption that H is a finitely projective K-module was used only in the proof of (v) $\Rightarrow$ (iii).

Proposition 5.3. *If the algebra* $\mathrm{St}(\mathfrak{p})$ *is semisimple for some* $\mathfrak{p} \in \mathrm{Spec}\, A$ *then there exists an integral* $\varphi : H \to A$ *such that* $\varphi(1) \notin \mathfrak{p}$. *If the algebras* $\mathrm{St}(\mathfrak{p})$ *are semisimple for all maximal ideals* $\mathfrak{p}$ *of* A *then there exists a total integral* $\varphi : H \to A$.

Proof. (i) Consider first a *preliminary step* in which we assume that K is a field and $\mathfrak{p}$ is a maximal ideal of A such that $A = K + \mathfrak{p}$. Then $k(\mathfrak{p}) \cong K$, and one has $O(\mathfrak{p}) = \delta_{\mathfrak{p}}(A)$. Let $I = \ker \delta_{\mathfrak{p}}$. The H-comodule algebras $O(\mathfrak{p})$ and A/I are isomorphic, whence the category $\mathscr{M}_{A/I}^H$ is equivalent to the category of $\mathrm{St}(\mathfrak{p})$-modules by

Proposition 1.6. As $\mathrm{St}(\mathfrak{p})$ is semisimple, all $\mathrm{St}(\mathfrak{p})$-modules are projective. It follows that so are all objects of $\mathscr{M}^H_{A/I}$ too. In particular, A/I is projective in $\mathscr{M}^H_{A/I}$. Then A/I is an injective H-comodule by Proposition 5.2. Hence A/I is an injective H^*-module. Since H^* is a Frobenius algebra, A/I is also a projective H^*-module. It follows that the canonical epimorphism of H^*-modules $A \to A/I$ splits, and so there exists an H-subcomodule $V \subset A$ such that $A = V \oplus I$. Now V is an injective H-comodule as it is isomorphic to A/I. Denote by $v \in V$ the element which projects to 1 in A/I. Clearly $v \in V^H$. Note that K is a trivial H-subcomodule of H. By injectivity of V the H-comodule homomorphism $K \to V$ such that $1 \mapsto v$ extends to an H-comodule homomorphism $\varphi : H \to V$ which can be regarded as an integral $H \to A$. We have $\varphi(1) = v$. By Lemma 3.1 $I \subset \mathfrak{p}$. It follows that $v \notin \mathfrak{p}$, and the required property of φ is fulfilled.

Consider now the *General case*. Let $\mathfrak{p}$ be given, and put $H' = k(\mathfrak{p}) \otimes H$. The hypotheses of the preliminary step are fulfilled for the H'-comodule algebra $A' = k(\mathfrak{p}) \otimes A$ over $k(\mathfrak{p})$ and its maximal ideal $\mathfrak{p}'$ defined in Lemma 5.1. It follows that there exists an integral $\psi : H' \to A'$ such that $\psi(1) \notin \mathfrak{p}'$. Taking the composite with the map $H \to H'$ defined by the rule $h \mapsto 1 \otimes h$, we obtain an integral $\chi : H \to A'$ satisfying $\chi(1) \notin \mathfrak{p}'$. Note that the H-comodule homomorphisms are precisely the H^*-module homomorphisms. By Lemma 1.3 the H^*-module H is finitely projective. Hence

$$\mathrm{Hom}_{H^*}(H, A') \cong k(\mathfrak{p}) \otimes \mathrm{Hom}_{H^*}(H, A).$$

If $\varphi : H \to A$ is an integral, then $1 \otimes \varphi$ corresponds under this isomorphism to the integral $\gamma \circ \varphi : H \to A'$ where $\gamma : A \to A'$ is defined by the rule $a \mapsto 1 \otimes a$ for $a \in A$. There exists therefore φ such that $(\gamma \circ \varphi)(1) \notin \mathfrak{p}'$. Since $\gamma^{-1}(\mathfrak{p}') = \mathfrak{p}$, we get $\varphi(1) \notin \mathfrak{p}$.

(ii) If $a \in A^H$ and $\varphi, \psi : H \to A$ are two integrals then $a\varphi$ and $\varphi + \psi$ are also integrals. In other words, the set $\mathrm{Com}(H, A)$ of all integrals $H \to A$ is an A^H-module in a natural way. One sees that the map $\mathrm{Com}(H, A) \to A$ such that $\varphi \mapsto \varphi(1)$ is a homomorphism of A^H-modules. Its image J is therefore an ideal of A^H. If $\mathrm{St}(\mathfrak{p})$ is semisimple for some $\mathfrak{p} \in \mathrm{Spec}\, A$ then $J \not\subset \mathfrak{p}$ by (i). It follows that $J = A$ as long as the algebras $\mathrm{St}(\mathfrak{p})$ are semisimple for all maximal ideals of A. In this case $1 \in J$, and we are done. $\square$

Remark. Conversely, if there exists an integral $\varphi : H \to A$ such that $\varphi(1) \notin \mathfrak{p}$, then it is possible to prove, using Proposition 1.6, that all left $k(\mathfrak{p}) \otimes H^*$-modules are semisimple $\mathrm{St}(\mathfrak{p})$-modules. I do not know if this suffices to assert that $\mathrm{St}(\mathfrak{p})$ is semisimple. Koppinen [17, Section 5] shows the semisimplicity of coideal subalgebras in finite-dimensional Hopf algebras under additional assumptions. If, however, H is commutative, then $\mathrm{St}(\mathfrak{p})$ is a Hopf subalgebra, and the conclusion is true. In this case one can add another equivalent condition to the list in Proposition 5.2:

(vii) *The algebras* $\mathrm{St}(\mathfrak{p})$ *are semisimple for all* $\mathfrak{p} \in \mathrm{Spec}\, A$.

We say that the Hopf algebra H is *geometrically cosemisimple* if for every ring homomorphism $K \to E$ into a field E the Hopf algebra $E \otimes H$ over E is cosemisimple, that is, the dual Hopf algebra $E \otimes H^*$ is semisimple.

Corollary 5.4. *H is geometrically cosemisimple if and only if H^* contains a right integral φ such that $\varphi(1) = 1$.*

Proof. Apply Proposition 5.3 to $A = K$ equipped with the trivial coaction of H, so that $K^H = K$. We have $O(\mathfrak{p}) = k(\mathfrak{p}) \otimes 1$, hence $\mathrm{St}(\mathfrak{p}) = k(\mathfrak{p}) \otimes H^*$ for each $\mathfrak{p} \in \mathrm{Spec}\, A$. If H is geometrically cosemisimple then the algebras $k(\mathfrak{p}) \otimes H^*$ are semisimple. In this case there exists a total integral $\varphi : H \to K$ which is none other but a right integral in H^*. Conversely, if H^* has a right integral φ satisfying $\varphi(1) = 1$, then so too does $E \otimes H^*$ for any ring homomorphism $K \to E$ into a field E. By Sweedler [29, Theorem 5.1.8] $E \otimes H^*$ is semisimple. □

As an example consider one special case: Suppose that $pK = 0$ where p is a prime integer. Let L be a p-Lie algebra over K whose underlying K-module is finitely projective. Denote by $u(L)$ the restricted universal enveloping algebra of L. Its underlying K-module is finitely projective as well [7, Chapter II, Section 7, Corollary 3.7]. Put $H = u(L)^*$ so that $H^* \cong u(L)$. Every homomorphism of p-Lie algebras $L \to \mathrm{Der}_K\, A$ into the p-Lie algebra of K-linear derivations of A gives rise to an action of $u(L)$ on A which makes A into a $u(L)$-module algebra, hence into an H-comodule algebra. If $\mathfrak{p} \in \mathrm{Spec}\, A$ then $\mathrm{St}(\mathfrak{p})$ is a Hopf subalgebra of $k(\mathfrak{p}) \otimes u(L) \cong u(k(\mathfrak{p}) \otimes L)$ since the latter Hopf algebra is cocommutative. Hence $\mathrm{St}(\mathfrak{p}) = u(L_{\mathfrak{p}})$ where $L_{\mathfrak{p}}$ is a $[p]$-closed subalgebra of the finite dimensional p-Lie algebra $k(\mathfrak{p}) \otimes L$ over $k(\mathfrak{p})$. In view of Lemma 5.1 $L_{\mathfrak{p}}$ coincides with the stabilizer of $\mathfrak{p}'$ with respect to the natural action of $k(\mathfrak{p}) \otimes L$ on $k(\mathfrak{p}) \otimes A$.

Corollary 5.5. *In order that there exist a total integral $u(L)^* \to A$ it is necessary and sufficient that $L_{\mathfrak{p}}$ be a torus for every maximal ideal $\mathfrak{p}$ of A.*

Proof. As was shown by Hochschild [15] $u(L_{\mathfrak{p}})$ is semisimple if and only if $L_{\mathfrak{p}}$ is a torus. Hence Proposition 5.3 and the remark following it applies. □

6. Weakly reductive coactions

We say that A is *weakly reductive* with respect to the coaction of H if for every H-costable ideal I of A the canonical map $\psi : A^H \to (A/I)^H$ is surjective.

Proposition 6.1. *A is weakly reductive with respect to coaction of H in any of the following three cases:*

(a) *A has invariant characteristic polynomials and $\mathrm{rk}_{\mathfrak{q}}\, H$ is invertible in A for every $\mathfrak{q} \in \mathrm{Spec}\, K$,*
(b) *there exists a total integral $H \to A$,*
(c) *A is H-reduced and $\mathrm{St}(\mathfrak{p})$ is semisimple for every maximal ideal $\mathfrak{p}$ of A which is not H-regular.*

Proof. Let I be an H-costable ideal of A.

(a) Denote by m the least common multiple of all $\mathrm{rk}_{\mathfrak{q}} H$ with $\mathfrak{q} \in \mathrm{Spec}\, K$. Proposition 2.6 shows that $m \cdot (A/I)^H \subset \mathrm{im}\, \psi$. The hypothesis of (a) implies that $m^{-1} \in A$, hence $m^{-1} \in A^H$. It follows that ψ is surjective.

(b) The surjectivity of ψ is a consequence of condition (v) in Proposition 5.2.

(c) For ψ to be surjective it is necessary and sufficient that so be its localizations $\psi_{\mathfrak{q}}$ at all maximal ideals $\mathfrak{q}$ of A^H. By Lemma 1.1 we may identify $\psi_{\mathfrak{q}}$ with the canonical map $(A_{\mathfrak{q}})^H \to (A_{\mathfrak{q}}/IA_{\mathfrak{q}})^H$. Replacing A with $A_{\mathfrak{q}}$, we may thus assume that the ring A^H is local with a maximal ideal $\mathfrak{q}$. If there exists an H-regular maximal ideal of A then all prime ideals of A are H-regular by Lemma 3.6, and the surjectivity of ψ follows from Theorem 4.3(ii). Otherwise the algebras $\mathrm{St}(\mathfrak{p})$ are semisimple for all maximal ideals of A, and there exists a total integral $H \to A$ by Proposition 5.3. In this case (b) applies. $\square$

Remark. Suppose that K is field. In this case the second part of (a) means that $\mathrm{char}\, K$ does not divide $\dim_K H$. Condition (b) is fulfilled, for instance, when H is cosemisimple.

Theorem 6.2. *If A is weakly reductive with respect to coaction of H then*:

(i) *A is integral over A^H.*

(ii) *If $\mathfrak{p} \in \mathrm{Spec}\, A$ and $\mathfrak{q} = \mathfrak{p} \cap A^H$, then $k(\mathfrak{p})$ is a finite extension of $k(\mathfrak{q})$ of degree $[k(\mathfrak{p}) : k(\mathfrak{q})] \leqslant \dim O(\mathfrak{p})$.*

(iii) *If A is Noetherian then so too is A^H and A is a finite A^H-module.*

(iv) *If A is Cohen–Macaulay then so too is A^H.*

Proof. (i) Denote by R the H-radical of A. As A/R is H-reduced, it has invariant characteristic polynomials by Theorem 2.5, and so A/R is integral over $(A/R)^H$ by Proposition 2.7. Since A is weakly reductive, we have $(A/R)^H = B/R$ where $B = A^H + R$. It follows that A is integral over B. All elements of R are nilpotent, hence integral over A^H. Then B is integral over A^H, and so too is A.

(ii) Let I be the largest H-costable ideal of A such that $I \subset \mathfrak{p}$. The H-comodule algebra $A' = A_{\mathfrak{q}}/IA_{\mathfrak{q}}$ is H-simple by Lemma 4.2. Letting $\mathfrak{p}' = \mathfrak{p}A_{\mathfrak{q}}/IA_{\mathfrak{q}}$ and $\mathfrak{q}' = \mathfrak{p}' \cap A'^H$, we have $k(\mathfrak{p}') \cong k(\mathfrak{p})$ and $k(\mathfrak{q}') \cong k(\mathfrak{q})$. The second isomorphism is a consequence of the surjectivity of the map $A^H \to (A/I)^H$. We may therefore replace A with A' and so assume that A is H-simple. Then the desired conclusion follows from Lemma 4.1. Indeed, A^H is a field, so that $\mathfrak{q} = (0)$ and $k(\mathfrak{q}) \cong A^H$. We have also $\dim_{A^H} A = \dim O(\mathfrak{p})$ and $k(\mathfrak{p}) \cong A/\mathfrak{p}$.

(iii) Suppose that A is not a finitely generated A^H-module. Since A is Noetherian, A contains an ideal I, maximal with respect to the properties that I is H-costable and A/I is not a finitely generated $(A/I)^H$-module. Replacing A with A/I, we may assume that A/J is a finitely generated $(A/J)^H$-module for every H-costable nonzero ideal J of A. Since the canonical map $A^H \to (A/J)^H$ is surjective, for any such a J

there exists a finitely generated A^H-submodule $F \subset A$ which is mapped onto the whole A/J under the projection $A \to A/J$, so that $A = F + J$.

Denote by R the H-radical of A. Suppose that $R \neq 0$. Then there exists a finitely generated A^H-submodule $F \subset A$ such that $A = F + R$. Let X be a finite set of generators for the A^H-module F. Since A is Noetherian, the ideal R of A has a finite set of generators, say Y. Denote by B the A^H-subalgebra of A generated by $X \cup Y$. As $F \subset B$ by construction, we have $A = B + R$. Since $Y \subset B$, we have also $R = (B + R)Y \subset B + R^2$. An easy induction shows that $R^{m-1} = (R^{m-1} \cap B) + R^m$ and $A = B + R^m$ for all $m > 0$. As R is a finitely generated nil ideal of A, there exists m such that $R^m = 0$. Thus $A = B$, and so A is finitely generated as an algebra over A^H. By (i) A is also a finitely generated A^H-module [4, Chapter V, Section 1, Proposition 4].

Suppose now that $R = 0$, that is, A is H-reduced. By Proposition 3.5 A contains an H-regular prime ideal $\mathfrak{p}$. Let $a_1, \dots, a_d \in A$, $s \in A^H$ and $n > 0$ be as in Lemma 4.6. The ideal $s^n A$ of A is H-costable and nonzero. Hence there exists a finitely generated A^H-submodule $F \subset A$ such that $A = F + s^n A$. From Lemma 4.6 it follows that $A = F + \sum A^H a_i$. Thus in both cases we have arrived at a contradiction.

We can conclude that A is a finitely generated A^H-module. By Eakin's theorem [12, Appendix of 21, 25] A^H is Noetherian.

(iv) By (iii) A^H is Noetherian. We have to prove that $A^H_{\mathfrak{q}}$ is Cohen–Macaulay for every $\mathfrak{q} \in \operatorname{Spec} A^H$. Replacing A with $A_{\mathfrak{q}}$, we may thus assume that the ring A^H is local with a maximal ideal $\mathfrak{q}$. If $\operatorname{Spec} A^H = \{\mathfrak{q}\}$ then A^H is Artinian, and we are done. Otherwise, let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be all minimal prime ideals of A. By the going-down property in Theorem 3.3 each $\mathfrak{p}_i \cap A^H$ is a minimal prime ideal of A^H, whence $\mathfrak{q} \not\subset \mathfrak{p}_i$. Then $\mathfrak{q} \not\subset \bigcup \mathfrak{p}_i$ [4, Chapter II, Section 1, Proposition 2]. The set of zero divisors in A coincides with $\bigcup \mathfrak{p}_i$ [21, (16.C)]. It follows that $\mathfrak{q}$ contains an element x which is not a zero divisor in A. The factor ring A/xA is Cohen–Macaulay of smaller Krull dimension than A. Furthermore, $(A/xA)^H \cong A^H/(xA \cap A^H)$ since A is weakly reductive. Suppose that $a \in A$ is an element such that $xa \in A^H$. Then $(x \otimes 1)\delta a = \delta(xa) = xa \otimes 1$. Since H is a flat K-module, $x \otimes 1$ is not a zero divisor in $A \otimes H$. So it follows that $\delta a = a \otimes 1$, i.e., $a \in A^H$. Thus $(A/xA)^H \cong A^H/xA^H$. If the ring A^H/xA^H is Cohen–Macaulay then so too is A^H since x is not a zero divisor in A^H [21, (16.A)]. So we may proceed by induction on $\dim A$. $\square$

Remark. If there exists a total integral $H \to A$ then A^H is an A^H-module direct summand of A. In this case (iv) follows from the Hochster–Eagon theorem [5, Theorem 6.4.5], [16, Proposition 12].

One may also note that all results of Section 3 are valid for a weakly reductive A without the assumption that A has invariant characteristic polynomials. Indeed, $\operatorname{Spec} A$ and $\operatorname{Spec} A^H$ are homeomorphic to $\operatorname{Spec} A/R$ and $\operatorname{Spec} (A/R)^H$, respectively, where R stands for the H-radical of A. So the proofs are obtained by passing to the H-reduced algebra A/R.

Suppose that $pK = 0$ where p is a prime integer and L is a finitely K-projective p-Lie algebra over K operating on A via K-linear derivations. Taking into account Corollary 5.5, we get

Corollary 6.3. *If A is Cohen–Macaulay and $L_{\mathfrak{p}}$ is a torus for every maximal ideal $\mathfrak{p}$ of A then the subring of L-invariants $A^L \subset A$ is Cohen–Macaulay.*

This generalizes [1, (3.1)], [2, (7.1)] where the invariants of a single derivation were considered under more restrictive assumptions on A.

Acknowledgments

The author gratefully acknowledges the support of the Alexander von Humboldt Foundation through the program of long-term cooperation.

References

[1] A.G. Aramova, Reductive derivations of local rings of characteristic p, J. Algebra 109 (1987) 394–414.
[2] A.G. Aramova, L.L. Avramov, Singularities of quotients by vector fields in characteristic p, Math. Ann. 273 (1986) 629–645.
[3] N. Bourbaki, Algèbre, Hermann, Paris, 1970 (Chapitres 1–3); Masson, Paris, 1981 (Chapitres 4–7).
[4] N. Bourbaki, Commutative Algebra, Springer, Berlin, 1989.
[5] W. Bruns, J. Herzog, Cohen–Macaulay Rings, Cambridge University Press, Cambridge, MA, 1993.
[6] S.U. Chase, M. Sweedler, Hopf Algebras and Galois Theory, in: Lecture Notes in Mathematics, Vol. 97, Springer, Berlin, 1969.
[7] M. Demazure, P. Gabriel, Groupes Algébriques I, Masson, Paris, 1970.
[8] D.E. Dobbs, I.J. Papick, Flat or open implies going down, Proc. Amer. Math. Soc. 65 (1977) 370–371.
[9] Y. Doi, Algebras with total integrals, Comm. Algebra 13 (1985) 2137–2159.
[10] Y. Doi, Hopf extensions of algebras and Maschke type theorems, Israel J. Math. 72 (1990) 99–108.
[11] Y. Doi, M. Takeuchi, Hopf–Galois extensions of algebras, the Miyashita–Ulbrich action, and Azumaya algebras, J. Algebra 121 (1989) 488–516.
[12] P.M. Eakin Jr., The converse to a well known theorem on Noetherian rings, Math. Ann. 177 (1968) 278–282.
[13] A. Grothendieck, J.A. Dieudonné, Éléments de géométrie algébrique. I, Springer, Berlin, 1971.
[14] W.J. Haboush, Reductive groups are geometrically reductive, Ann. Math. 102 (1975) 67–83.
[15] G.P. Hochschild, Representations of restricted Lie algebras of characteristic p, Proc. Amer. Math. Soc. 5 (1954) 603–605.
[16] M. Hochster, J.A. Eagon, Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci, Amer. J. Math. 93 (1971) 1020–1058.
[17] M. Koppinen, Coideal subalgebras in Hopf algebras: freeness, integrals, smash products, Comm. Algebra 21 (1993) 427–444.
[18] H.F. Kreimer, M. Takeuchi, Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J. 30 (1981) 675–692.
[19] R.G. Larson, D.E. Radford, Semisimple Hopf algebras, J. Algebra 171 (1995) 5–35.
[20] A. Masuoka, Freeness of Hopf algebras over coideal subalgebras, Comm. Algebra 20 (1992) 1353–1373.

[21] H. Matsumura, Commutative Algebra, 2nd Edition, Benjamin, New York, 1980.
[22] S. Montgomery, Hopf algebras and their actions on rings, in: CBMS Regional Conference Series in Mathematics, Vol. 82, American Mathematical Society, Providence, RI, 1993.
[23] D. Mumford, Geometric Invariant Theory, in: Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 34, Springer, Berlin, 1965.
[24] D. Mumford, Abelian Varieties, Oxford University Press, Oxford, 1970.
[25] M. Nagata, A type of subrings of a noetherian ring, J. Math. Kyoto Univ. 8 (1968) 465–467.
[26] B. Pareigis, When Hopf algebras are Frobenius algebras, J. Algebra 18 (1971) 588–596.
[27] H.-J. Schneider, Principal homogeneous spaces for arbitrary Hopf algebras, Israel J. Math. 72 (1990) 167–195.
[28] S. Skryabin, Invariants of finite group schemes, J. London Math. Soc. 65 (2002) 339–360.
[29] M.E. Sweedler, Hopf Algebras, Benjamin, New York, 1969.
[30] K.-H. Ulbrich, Galoiserweiterungen von nicht–kommutativen Ringen, Comm. Algebra 10 (1982) 655–672.
[31] W.C. Waterhouse, Geometrically reductive affine group schemes, Arch. Math. 62 (1994) 306–307.
[32] S. Zhu, Integrality of module algebras over its invariants, J. Algebra 180 (1996) 187–205.